PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-224409
(43)Date of publication of application : 21.08.1998

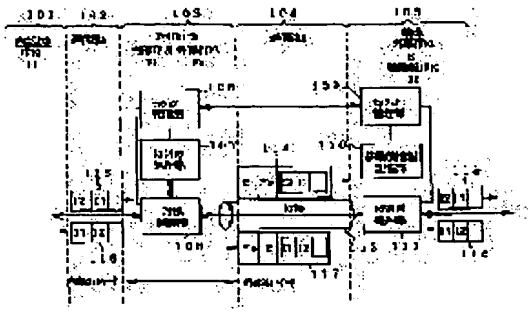
(51)Int.Cl. H04L 12/66
G06F 13/00
G06F 13/00

(21)Application number : 09-024677
(22)Date of filing : 07.02.1997

(71)Applicant : OKI ELECTRIC IND CO LTD
(72)Inventor : TORII TAKASHI
NAKAGAWA SATOSHI

(54) COMMUNICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To continuously enjoy the service within a range of the application right received before a terminal set at a position in an internal network is moved to an external network by storing the terminal address that is assigned before the movement of the terminal or previously assigned in the internal network.
SOLUTION: When the communication is started between an internal host 101 and a terminal 105, a session management part 106 communicates with a session management part 109 to perform the authentication and key exchange to the terminal 105. The part 109 notifies the part 106 of a fact that the terminal 105 moved to an external network and an external address is equal to E and I2 after and before movement of the terminal 105 respectively. Thus, an access control part 108 relays a packet 113 between the host 101 and the terminal 105. The receiving and transmitting destination addresses of the packet 113 sent to the terminal 105 from the host 101 are equal to I2 and I1 respectively.



LEGAL STATUS

[Date of request for examination] 15.12.2000
[Date of sending the examiner's decision of rejection] 07.12.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

THIS PAGE BLANK (USPTO)

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－224409

(43)公開日　平成10年(1998)８月21日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　11/20	Ｂ
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ａ
	３５４		３５４Ａ

審査請求　未請求　請求項の数22　ＯＬ　（全 30 頁）

(21)出願番号　特願平9－24677

(22)出願日　平成９年(1997)２月７日

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号

(72)発明者　烏居　肖史
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内

(72)発明者　中川　聰
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内

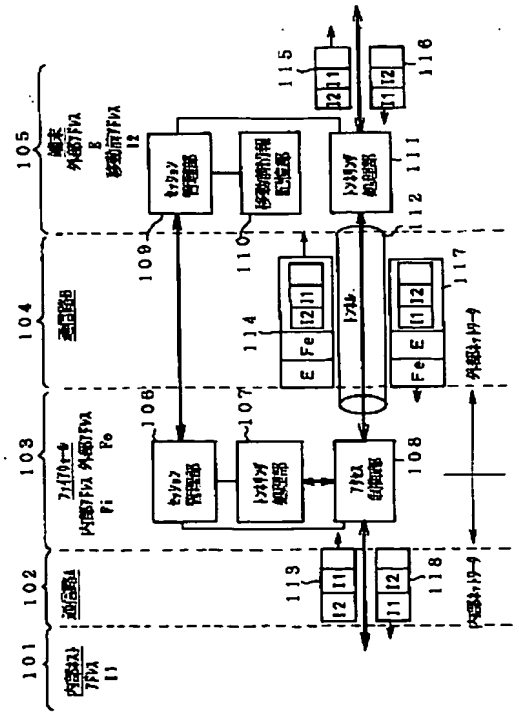
(74)代理人　弁理士　工藤　宜幸

(54)【発明の名称】　通信システム

(57)【要約】

【課題】　内部ネットワークに位置する端末を外部ネットワークへ移動させると、端末のアドレスに変化が生じるため、移動前の利用権限ではサービスを受け得ない。

【解決手段】　外部ネットワークの端末に、移動前に又は予め内部ネットワークにおいて割り当てられていた端末アドレスを記憶するアドレス記憶手段を備えるようにする。これにより、外部ネットワークに位置する端末であっても内部ネットワークで割り当てられた端末アドレスを記憶する端末については、内部ホスト側において、当該端末に提供し得るサービスの利用権限を判別することが可能とできる。



1

【特許請求の範囲】

【請求項１】　外部ネットワークに位置する端末が、ファイアウォールを介して内部ネットワークの内部ホストと通信する形態の通信システムにおいて、

上記端末は、移動前に又は予め内部ネットワークにおいて割り当てられた端末アドレスを記憶するアドレス記憶手段を備えることを特徴とする通信システム。

【請求項２】　上記端末及び上記ファイアウォールは、当該端末が内部ネットワークから外部ネットワークへ移動した場合に、上記アドレス記憶手段が記憶している端末アドレスと同一のアドレスを有するパケットを、カプセル化後、上記端末及びファイアウォールの間に形成したトンネルを介して入出力するトンネリング処理手段を備えることを特徴とする請求項１に記載の通信システム。

【請求項３】　上記端末及び上記内部ホストは、当該端末が内部ネットワークから外部ネットワークへ移動した場合に、上記アドレス記憶手段が記憶している端末アドレスと同一のアドレスを有するパケットを、カプセル化後、上記端末及び内部ホスト間に形成したトンネルを介して入出力するトンネリング処理手段を備えることを特徴とする請求項１に記載の通信システム。

【請求項４】　上記内部ネットワークにおける各サブネットのサブネット管理サーバは、上記端末が内部ネットワークから外部ネットワークへ移動した場合に、上記アドレス記憶手段が記憶している端末アドレスと同一のアドレスを有するパケットを、カプセル化後、当該サブネット管理サーバと上記端末との間に形成したトンネルを介して入出力するトンネリング処理手段を備えることを特徴とする請求項１に記載の通信システム。

【請求項５】　上記ファイアウォールはトンネルの内部に位置し、当該ファイアウォールは、上記パケットのヘッダのアドレスを書き換えるヘッダアドレス書換手段を備えることを特徴とする請求項３又は４に記載の通信システム。

【請求項６】　上記ファイアウォールは、内部ネットワークに接続しているネットワーク・インターフェースのアドレスを複数有することを特徴とする請求項５に記載の通信システム。

【請求項７】　上記ファイアウォールは、内部ネットワークに接続しているネットワーク・インターフェースのアドレスを複数有し、かつ、外部ネットワークに接続しているネットワーク・インターフェースのアドレスを複数有することを特徴とする請求項５に記載の通信システム。

【請求項８】　上記ファイアウォールは、パケットのヘッダに記録されているセキュリティ関連情報に基づいて、上記パケットのヘッダのアドレスを書き換えることを特徴とする請求項５に記載の通信システム。

【請求項９】　上記ファイアウォールは、パケットのヘッダに記録されている、パケットが通過するトンネルの両端アドレスを表すフィールドの値に基づいて、上記パケットのヘッダのアドレスを書き換えることを特徴とする請求項５に記載の通信システム。

2

【請求項１０】　内部ネットワーク内のあるサブネットに位置する端末が、当該ネットワーク内で内部ホストと通信する形態の通信システムにおいて、

上記端末は、同じネットワーク内のあるサブネットから他のサブネットへ移動した後も、移動前に割り当てられた端末アドレスを記憶し続けるアドレス記憶手段を備え、かつ、上記端末及び上記内部ホストは、当該移動があった場合に、上記アドレス記憶手段が記憶している移動前の端末アドレスと同一のアドレスを有するパケットを、カプセル化後、上記端末及び内部ホストの間に形成したトンネルを介して入出力するトンネリング処理手段を備えることを特徴とする通信システム。

【請求項１１】　内部ネットワーク内のあるサブネットに位置する端末が、当該ネットワーク内の内部ホストと通信する形態の通信システムにおいて、

上記端末は、同一ネットワーク内のあるサブネットから他のサブネットへ移動した後も、移動前に割り当てられた端末アドレスを記憶し続けるアドレス記憶手段を備え、かつ、上記端末及び当該端末が移動前に位置したサブネットのサブネット管理サーバは、当該移動があった場合に、上記アドレス記憶手段が記憶している移動前の端末アドレスと同一のアドレスを有するパケットを、カプセル化後、上記端末及びサブネット管理サーバ間に形成したトンネルを介して入出力するトンネリング処理手段を備えることを特徴とする通信システム。

【請求項１２】　内部ネットワーク内のあるサブネットに位置する端末が、当該ネットワーク内の内部ホストと通信する形態の通信システムにおいて、

上記端末は、同一ネットワーク内のあるサブネットから他のサブネットへ移動した後も、移動前に割り当てられた端末アドレスを記憶し続けるアドレス記憶手段を備え、かつ、上記端末の移動の前後に係る各サブネットのサブネット管理サーバは、当該移動があった場合に、上記アドレス記憶手段が記憶している移動前の端末アドレスと同一のアドレスを有するパケットを、カプセル化後、当該サブネット管理サーバ間に形成したトンネルを介して入出力するトンネリング処理手段を備えることを特徴とする通信システム。

【請求項１３】　上記ファイアウォールは、内部ネットワークから外部ネットワークへ移動した端末に対して外部ネットワークが割り当てた端末アドレスを記憶するアドレス記憶手段を備えることを特徴とする請求項１～９のいずれかに記載の通信システム。

【請求項１４】　上記内部ネットワーク内のサブネット管理サーバは、内部ネットワークから外部ネットワークへ移動した端末に対して外部ネットワークが割り当てた

端末アドレスを記憶するアドレス記憶手段を備えることを特徴とする請求項１～９のいずれかに記載の通信システム。

【請求項１５】　上記トンネルの両端位置に、上記パケットを暗号処理する暗号処理手段を備えることを特徴とする請求項１～１４のいずれかに記載の通信システム。

【請求項１６】　上記トンネルの両端位置を除く内部位置に、上記パケットを暗号処理する暗号処理手段を備えることを特徴とする請求項１～１４のいずれかに記載の通信システム。

【請求項１７】　上記暗号処理手段は、上記パケットのヘッダのアドレスに応じて、暗号処理のアルゴリズムを、１つ以上の暗号処理のアルゴリズムと恒等写像のうちのいずれかに切り替えることを特徴とする請求項１５又は１６に記載の通信システム。

【請求項１８】　上記暗号処理手段は、上記パケットのヘッダに記憶されているセキュリティ関連情報に応じて、暗号処理のアルゴリズムを、１つ以上の暗号処理のアルゴリズムと恒等写像のうちのどれかに切り替えることを特徴とする請求項１５又は１６に記載の通信システム。

【請求項１９】　上記トンネルの両端位置に、パケットを認証処理する認証処理手段を備えることを特徴とする請求項１～１４のいずれかに記載の通信システム。

【請求項２０】　上記トンネルの両端位置を除く内部位置に、パケットを認証処理する認証処理手段を備えることを特徴とする請求項１～１４のいずれかに記載の通信システム。

【請求項２１】　上記認証処理手段は、上記パケットのヘッダのアドレスに応じて、パケットの認証処理のアルゴリズムを変更することを特徴とする請求項１９又は２０に記載の通信システム。

【請求項２２】　上記認証処理手段は、上記パケットのヘッダに記憶されているセキュリティ関連情報に応じて、パケットの認証処理のアルゴリズムを変更することを特徴とする請求項１９又は２０に記載の通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、通信システムに関し、特に、ファイアウォールを介して内外のネットワーク間で通信を行うシステムに好適なものである。

【０００２】

【従来の技術】

文献名：R. Atkinson, "Security Architecture for the Internet Protocol ", RFC1825, August 1995

従来、この種の通信システムで用いられる通信方式として、上記文献に開示されている通信方式がある。この通信方式は、外部ネットワークのホスト（外部ホスト）がファイアウォールを介して内部ネットワークのホスト

（内部ホスト）と通信する場合に、ファイアウォールが外部ホストを認証して鍵交換した後、当該ファイアウォールと外部ホストの間でパケットの暗号処理を行ってトンネリングすることで、外部ネットワークでの盗聴、改竄、なりすましを防止するものである。

【０００３】ここで、トンネリングとは、ＷＩＤＥプロジェクト“１９９４年度ＷＩＤＥプロジェクト研究報告書”p137 にも示されているように、ネットワーク層のプロトコル（例えばＩＰ：Internet Protocol）を伝達するために、同じネットワーク層のプロトコル（例えばＩＰ）をデータリンク層のプロトコルとみなして利用する技術をいう。また、トンネルとは、通信路のうちトンネリングを適用する部分をいう。

【０００４】図２に、トンネル内を伝送されるパケットの構造例を示す。図２の場合、「パケットＢ」２０２が、「パケットＡ」２０１のペイロード２０４に格納されているが、これは、「パケットＡ」２０１が、「パケットＢ」２０２をカプセル化（encapsulation）している状態を表している。なお、あるパケットのペイロードからカプセル化されているパケットを抽出する処理を、以下、脱カプセル化（decapsulation）という。

【０００５】ところで、上記文献の通信方式では、次に示す(a)～(c)の手段が必要になる。(a)の手段は、ファイアウォールが外部ホストを認証し鍵の交換を行うための手段（以下、セッション管理部という。）である。この手段は、ファイアウォールと外部ホストのそれぞれに必要とされる。(b)の手段は、ファイアウォールと外部ホストとの間でパケットを暗号処理しトンネリングするための手段（以下、トンネリング処理部という。）である。この手段も、ファイアウォールと外部ホストのそれぞれに必要とされる。(c)の手段は、アクセスを許可したパケットのみを中継しその他のパケットは遮断することにより、外部ネットワークから内部ネットワークへの不正なアクセスを防止するための手段（以下、アクセス制御部と呼ぶ。）である。この手段は、内部ネットワークと外部ネットワークの境界に設けられているファイアウォールに必要とされる。

【０００６】従って、上記文献の通信方式を用いる通信システムは、図３に示す構成となる。なお、上記文献には係る構成は示されていないので、図３は、必要とされる手段を基に作成したものである。

【０００７】このシステムは、内部ホスト３０１、「通信路Ａ」３０２、ファイアウォール３０３、「通信路Ｂ」３０４、外部ホスト３０５からなる。このうち、「通信路Ａ」３０２は、内部ホスト３０１とファイアウォール３０３間の通信路である。「通信路Ａ」３０２は、内部ネットワークの通信路に当たる。一方、「通信路Ｂ」３０４は、ファイアウォール３０３と外部ホスト３０５間の通信路である。「通信路Ｂ」３０４は、外部ネットワークの通信路に当たる。ファイアウォール３０

３は、前述したように(a) ～(c) の３つの手段、セッション管理部３０６、トンネリング処理部３０７、アクセス制御部３０８からなる。また、外部ホスト３０５は、前述した(a) 及び(b) の２つの手段、セッション管理部３０９、トンネリング処理部３１０からなる。ところで、ファイアウォール３０３と外部ホスト３０５の間にはトンネル３１１がある。

【０００８】次に、かかる構成のシステムにおいて実行される通信動作を説明する。まず、内部ホスト３０１から外部ホスト３０５に対してパケットを送信する場合、ファイアウォール３０３が、パケット３１２を暗号処理し、さらに、図２のようにカプセル化する。カプセル化されたパケット３１２はパケット３１３として、トンネル３１１を伝送され外部ホスト３０５に達する。外部ホスト３０５は、これを脱カプセル化し、パケット３１４を得る。

【０００９】この反対に、外部ホスト３０５から内部ホスト３０１にパケットを送信する場合、外部ホスト３０５が、パケット３１５を暗号処理しパケット３１６のようにカプセル化する。このパケット３１６は、トンネル３１１を介してファイアウォール３０３に達し、ここで脱パケット化されて内部ホスト３０１にパケット３１７として与えられる。

【００１０】以上のようにして、双方向の通信がなされる。

【００１１】

【発明が解決しようとする課題】しかしながら、上記文献の通信方式の場合、内部ネットワーク上に位置する端末を、何らかの事情で外部ネットワーク上へ移動させた場合、以下に示す問題が生じてしまう。

【００１２】一般に、サービスを提供するアプリケーションは、サービスを要求しているホストのアドレスに基づいて、サービスの利用権限を求める。従って、内部ネットワーク上に位置する端末を、外部ネットワーク上へ移動すると、端末のアドレスが変化するので、端末は内部ホストが提供するサービスを移動前のサービス利用権限では利用できなくなってしまう。ここで、サービス利用権限には、例えば、サービスの利用を許可すること、又は、サービスの利用を禁止すること、サービスをある品質で許可することなどがある。

【００１３】本発明は以上の課題を考慮してなされたもので、内部ネットワーク上に位置していた端末を外部ネットワーク上へ移動しても、移動前に提供を受けることができたサービス利用権限の範囲内で引き続きサービスを享受できるようにするリモートアクセス通信システムを提供しようとするものである。

【００１４】

【課題を解決するための手段】

(A) かかる課題を解決するため第１の発明においては、外部ネットワークに位置する端末が、ファイアウォールを介して内部ネットワークの内部ホストと通信する形態の通信システムにおいて、以下の手段を備えたことを特徴とする。

【００１５】すなわち、端末は、移動前に又は予め内部ネットワークにおいて割り当てられた端末アドレスを記憶するアドレス記憶手段を備えたことを特徴とする。

【００１６】このように、第１の発明における通信システムによれば、外部ネットワークに位置する端末であっても内部ネットワークで割り当てられた端末アドレスを記憶する端末については、内部ホスト側において、当該端末に提供し得るサービスの利用権限を判別することが可能となる。これにより、特定の端末については、外部ネットワークに位置する場合にも、内部ネットワークに位置する場合と同じ利用権限でのサービスを受けることができる。

【００１７】(B) また、第２の発明においては、内部ネットワーク内のあるサブネットに位置する端末が、当該ネットワーク内で内部ホストと通信する形態の通信システムにおいて、以下の手段を備えることを特徴とする。

【００１８】すなわち、端末は、同じネットワーク内のあるサブネットから他のサブネットへ移動した後も、移動前に割り当てられた端末アドレスを記憶し続けるアドレス記憶手段を備え、かつ、端末及び内部ホストは、当該移動があった場合に、アドレス記憶手段が記憶している移動前の端末アドレスと同一のアドレスを有するパケットを、カプセル化後、端末及び内部ホストの間に形成したトンネルを介して入出力するトンネリング処理手段を備えることを特徴とする。

【００１９】このように、第２の発明における通信システムによれば、内部ネットワーク内であるサブネットから他のサブネットに端末が移動した場合にも、移動前における端末アドレスを端末が記憶しているので、内部ホスト側において、当該端末に提供し得るサービスの利用権限を判別することが可能となる。これにより、特定の端末については、他のサブネットに移動した場合にも、移動前のサブネットで許容されていたのと同じ利用権限でサービスを受けることができる。

【００２０】(C) さらに、第３の発明においては、内部ネットワーク内のあるサブネットに位置する端末が、当該ネットワーク内の内部ホストと通信する形態の通信システムにおいて、以下の手段を備えることを特徴とする。

【００２１】すなわち、端末は、同一ネットワーク内のあるサブネットから他のサブネットへ移動した後も、移動前に割り当てられた端末アドレスを記憶し続けるアドレス記憶手段を備え、かつ、端末及び当該端末が移動前に位置したサブネットのサブネット管理サーバは、当該移動があった場合に、アドレス記憶手段が記憶している移動前の端末アドレスと同一のアドレスを有するパケットを、カプセル化後、端末及びサブネット管理サーバ間

に形成したトンネルを介して入出力するトンネリング処理手段を備えることを特徴とする。

【００２２】このように、第３の発明における通信システムによれば、端末とサブネット管理サーバとの間にトンネルを設けているので、内部ホストごとに各端末までのトンネルを設けなくて良くなる。

【００２３】(D) さらに、第４の発明においては、内部ネットワーク内のあるサブネットに位置する端末が、当該ネットワーク内の内部ホストと通信する形態の通信システムにおいて、以下の手段を備えることを特徴とする。

【００２４】すなわち、端末は、同一ネットワーク内のあるサブネットから他のサブネットへ移動した後も、移動前に割り当てられた端末アドレスを記憶し続けるアドレス記憶手段を備え、かつ、端末の移動の前後に係る各サブネットのサブネット管理サーバは、当該移動があった場合に、アドレス記憶手段が記憶している移動前の端末アドレスと同一のアドレスを有するパケットを、カプセル化後、当該サブネット管理サーバ間に形成したトンネルを介して入出力するトンネリング処理手段を備えることを特徴とする。

【００２５】このように、第４の発明における通信システムによれば、サブネット管理サーバ間にトンネルを設けるので、端末がトンネリング処理をせずに済み、その分、端末の負荷を軽減できるという効果が得られる。

【００２６】

【発明の実施の形態】

（Ａ）各実施形態で用いるパケットの構造

まず、後述する各実施形態において使用されるパケットの基本構造を説明する。図４は、トンネルを介して送受されるパケットの構造を表した図である。この図４は、「パケットＢ」４０２が、「パケットＡ」４０１のペイロードに格納され、カプセル化（encapsulation）されている状態を表している。ここで、「パケットＡ」の受信先アドレス４０３と「パケットＡ」の送信元アドレス４０４が「パケットＡ」のヘッダを表し、「パケットＢ」の受信先アドレス４０５と「パケットＢ」の送信元アドレス４０６が「パケットＢ」のヘッダを表している。

【００２７】ここで、「パケットＢ」を端末へ入力する場合は、「パケットＢ」の受信先アドレス４０５に書き込まれているアドレスが、外部ネットワーク上でのアドレスではなく、予め内部ネットワークで各端末に割り当てられた内部ネットワーク上でのアドレス（内部ネットワークから外部ネットワークへ移動する場合における移動前のアドレスを含む）が書き込まれている。各実施形態では、このアドレスを用いた通信システムについて説明する。

【００２８】また、一部実施形態（第５の実施形態及び第１０の実施形態）においては、図５に示す構造のパケットを使用する。この図５の場合も、トンネルを介して送受されるパケットの構造を表した図であり、「パケットＢ」５０２が、「パケットＡ」５０１のペイロードに格納され、カプセル化（encapsulation）されている状態を表している。図５のパケットが図４のパケットと異なる点は、「パケットＡ」のヘッダが、「パケットＡ」の受信先アドレス５０３と「パケットＡ」の送信元アドレス５０４に加えて、「パケットＡ」のＳＰＩ（Security ParametersIndex）を有する点である。ここで、ＳＰＩは、使用する暗号アルゴリズムや鍵等のセキュリティに関するパラメータを表すものである。なお、「パケットＢ」のヘッダの構造は同じであり、「パケットＢ」を端末へ入力する場合は、「パケットＢ」の受信先アドレス５０５には、予め内部ネットワークで各端末に割り当てられた内部ネットワーク上でのアドレス（内部ネットワークから外部ネットワークへ移動する場合における移動前のアドレスを含む）が書き込まれている。

【００２９】（Ｂ）第１の実施形態

以下、第１の実施形態に係る通信システムを、図面を参照しながら説明する。

【００３０】（Ｂ－１）第１の実施形態の構成

図１は、第１の実施形態の構成図である。この通信システムは、内部ホスト１０１、「通信路Ａ」１０２、ファイアウォール１０３、「通信路Ｂ」１０４、端末１０５からなる。因みに、従来技術で説明した図３の場合には、外部ネットワーク側の受信先が外部ホスト３０５となっていたが、この実施形態の場合には端末１０５が接続されている。

【００３１】ここで、「通信路Ａ」１０２は、内部ホスト１０１とファイアウォール１０３の間の通信路である。「通信路Ａ」１０２は、内部ネットワークの通信路である。「通信路Ｂ」１０４は、ファイアウォール１０３と端末１０５の間の通信路である。「通信路Ｂ」１０４は、外部ネットワークの通信路である。

【００３２】本実施形態に係るファイアウォール１０３は、セッション管理部１０６、トンネリング処理部１０７、アクセス制御部１０８の各構成要素を有してなる。

【００３３】本実施形態に係る端末１０５は、セッション管理部１０９、移動前情報記憶部１１０、トンネリング処理部１１１の各構成要素を有してなる。このうち、移動前情報記憶部１１０は、後述する移動前アドレスＩ２の記憶に用いられる。

【００３４】なお、ファイアウォール１０３と端末１０５の間にトンネル１１２を設けることにする。

【００３５】内部ホスト１０１は、端末１０５のアドレスとして移動前アドレスＩ２を使用して、パケットを「通信路Ａ」１０２と送受信する。端末１０５は、端末１０５のアドレスとして移動前アドレスＩ２を使用して、パケットをトンネリング処理部１１１と入出力する。

【００３６】セッション管理部１０６とセッション管理部１０９は、互いに通信し、端末１０５の認証と鍵交換をする。セッション管理部１０９は、セッション管理部１０６へ、端末１０５が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であることを通知する。

【００３７】トンネリング処理部１０７は、セッション管理部１０６が交換した鍵を使用して、端末１０５宛てのパケットを暗号処理してカプセル化する。また、トンネリング処理部１０７は、内部ホスト１０１宛てのパケットを脱カプセル化し復号処理する。

【００３８】トンネリング処理部１１１は、セッション管理部１０９が交換した鍵を使用して、内部ホスト１０１宛てのパケットを暗号処理しカプセル化する。また、トンネリング処理部１１１は端末１０５宛てのパケットを脱カプセル化し復号処理する。

【００３９】アクセス制御部１０８は、受信するパケットが、内部ホスト１０１と端末１０５の間の通信のパケットであるかを判定する。アクセス制御部１０８は、内部ホスト１０１と端末１０５の間の通信のパケットを、トンネリング処理部１０７へ入力してパケットを加工し、中継する。アクセス制御部１０８は、内部ホスト１０１と端末１０５の間の通信ではないパケットを、中継しない。

【００４０】内部ホスト１０１のアドレスは、Ｉ１である。内部ネットワークに接続しているファイアウォール１０３のネットワーク・インターフェースのアドレスはＦｉである。外部ネットワークに接続しているファイアウォール１０３のネットワーク・インターフェースのアドレスはＦｅである。端末１０５のアドレスは、Ｅである。外部ネットワークへの移動前の端末１０５の内部ネットワークでのアドレス（移動前アドレス）はＩ２である。

【００４１】（Ｂ－２）第１の実施形態の通信動作

続いて、図１に示す通信システムによって実現される通信動作を説明する。

【００４２】（Ｂ－２－１）通信開始前の動作

まず、内部ホスト１０１と端末１０５が通信を開始するまでの動作を説明する。これには、セッション管理部１０６とセッション管理部１０９とが通信し、端末１０５の認証と鍵交換を行う。セッション管理部１０９は、セッション管理部１０６へ、端末１０５が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であることを通知する。これにより、アクセス制御部１０８は、内部ホスト１０１と端末１０５の間のパケットを中継するようになる。

【００４３】（Ｂ－２－２）通信開始後の動作

次に、内部ホスト１０１と端末１０５が通信をする時の動作を説明する。

【００４４】なお、内部ホスト１０１から端末１０５へ伝送されるパケット１１３の受信先アドレスはＩ２、送信元アドレスはＩ１となる。また、このパケット１１３をカプセル化したパケット１１４の受信先アドレスはＥ、送信元アドレスはＦｅとなる。これを脱パケット化した後のパケット１１５は、パケット１１３と同一となる。

【００４５】一方、端末１０５から内部ホスト１０１へ伝送されるパケット１１６の受信先アドレスはＩ１、送信元アドレスはＩ２となる。また、このパケット１１６をカプセル化したパケット１１７の受信先アドレスはＦｅ、送信元アドレスはＥとなる。これを脱パケット化した後のパケット１１８は、パケット１１６と同一となる。

【００４６】（Ｂ－２－２－１）内部ホストから端末への送信

まず、内部ホスト１０１から端末１０５にパケットを送信する場合の動作を説明する。

【００４７】内部ホスト１０１は、「通信路Ａ」１０２に対してパケット１１３を送信する。

【００４８】ファイアウォール１０３のアクセス制御部１０８は、「通信路Ａ」１０２からパケット１１３を受信する。アクセス制御部１０８は、そのヘッダから、パケット１１３は内部ホスト１０１と端末１０５間のパケットであると判定する。アクセス制御部１０８は、パケット１１３をトンネリング処理部１０７へ与える。トンネリング処理部１０７は、セッション管理部１０６が交換した鍵を使用して、パケット１１３を暗号処理してカプセル化し、パケット１１４を得る。この時、パケット１１３の受信先アドレスがＩ２であるので、パケット１１４の受信先アドレスをＥとする。かかる後、トンネリング処理部１０７は、パケット１１４をアクセス制御部１０８に与える。アクセス制御部１０８は、このパケット１１４を「通信路Ｂ」１０４へ送信する。

【００４９】端末１０５のトンネリング処理部１１１は、「通信路Ｂ」１０４からパケット１１４を受信する。トンネリング処理部１１１は、セッション管理部１０９が交換した鍵を使用して、パケット１１４を脱カプセル化し復号処理し、パケット１１５を得る。端末１０５は、トンネリング処理部１１１からパケット１１５を得る。

【００５０】（Ｂ－２－２－２）端末から内部ホストへの送信

逆に、端末１０５から内部ホスト１０１にパケットを送信する場合の動作を説明する。

【００５１】端末１０５は、パケット１１６をトンネリング処理部１１１へ入力する。トンネリング処理部１１１は、セッション管理部１０９が交換した鍵を使用して、パケット１１６を暗号処理してカプセル化し、パケット１１７を得る。トンネリング処理部１１１は、「通信路Ｂ」１０４へパケット１１７を送信する。

【００５２】ファイアウォール１０３のアクセス制御部１０８は、「通信路Ｂ」１０４からパケット１１７を受信する。アクセス制御部１０８は、パケット１１７は内部ホスト１０１と端末１０５の間のパケットであると判定する。アクセス制御部１０８は、パケット１１７をトンネリング処理部１０７へ入力する。トンネリング処理部１０７は、セッション管理部１０６が交換した鍵を使用して、パケット１１７を脱カプセル化し復号処理し、パケット１１８を得る。トンネリング処理部１０７は、パケット１１８をアクセス制御部１０８へ出力する。アクセス制御部１０８は、「通信路Ａ」１０２へパケット１１８を送信する。

【００５３】内部ホスト１０１は、パケット１１８を受信する。

【００５４】（Ｂ－２－３）通信終了動作

内部ホスト１０１と端末１０５が通信を終了する場合の動作を説明する。

【００５５】ファイアウォール１０３が通信の終了を要求する場合には、セッション管理部１０６がセッション管理部１０９に通信の終了を要求する。これに対して、端末１０５が通信の終了を要求する場合には、セッション管理部１０９がセッション管理部１０６に通信の終了を要求する。

【００５６】ファイアウォール１０３が「通信路Ｂ」１０４から受信するパケットには、アクセス制御部１０６が受信するパケットとセッション管理部１０６が受信するパケットがある。ファイアウォール１０３は、パケットのヘッダのうちアドレス以外の値により、どちらのパケットであるかを判定する。端末１０５が「通信路Ｂ」１０４から受信するパケットについても同様である。

【００５７】（Ｂ－２－４）内部ネットワークに対するサービスの提供

ファイアウォール１０３が内部ネットワーク向けにサービスを提供している場合について説明する。

【００５８】この場合は、アクセス制御部１０８は、「通信路Ａ」１０２と送受信するパケット（パケット１１３とパケット１１８）を、ファイアウォール１０３と入出力する。

【００５９】（Ｂ－３）第１の実施形態の効果

以上のように、第１の実施形態によれば、ファイアウォールと外部の端末との間にトンネルを設け、そのトンネルにおいて、端末アドレスに移動前アドレスを使用するパケットをカプセル化するようにしたので、内部ネットワークに位置する端末を外部ネットワークへ移動しても、内部ホストに対しては、端末のアドレスが外部ネットワークへの移動前後で変化していないようにみなせるので、端末は内部ホストが提供するサービスを移動前のサービス利用権限で利用できるという効果が得られる。

【００６０】また、これらサービスは、パケット伝送により実現されるので、複数の内部ホスト１０１と複数の端末１０５間において同時通信を実現できる。

【００６１】（Ｃ）第２の実施形態

続いて、第２の実施形態を説明する。ところで、前述の第１の実施形態が有効に機能するには、内部ネットワークにおいて、受信先アドレスが端末の移動前アドレスＩ２であるパケットがファイアウォールに届かなければならず、届かない場合には外部ネットワークに移動した端末との間で通信できない。例えば、内部ホストと移動前の端末との間の経路にファイアウォールが位置しない場合には、ルータの経路制御テーブルを変更しないと、受信先アドレスが端末の移動前アドレスＩ２であるパケットをファイアウォールに届けることができない。そこで、次の実施形態を考える。

【００６２】（Ｃ－１）第２の実施形態の構成

図６は、第２の実施形態の構成図である。この通信システムは、内部ホスト６０１、「通信路Ａ」６０２、ファイアウォール６０３、「通信路Ｂ」６０４、端末６０５からなる。ここで、「通信路Ａ」６０２は、内部ホスト６０１とファイアウォール６０３の間の通信路であり、内部ネットワークの通信路である。「通信路Ｂ」６０４は、ファイアウォール６０３と端末６０５の間の通信路である。「通信路Ｂ」６０４は、外部ネットワークの通信路である。

【００６３】この実施形態では、第１の実施形態においてはファイアウォールに設けられていた３つの構成要素のうち２つの構成要素が内部ホスト６０１側に設けるようにしている。すなわち、本実施形態に係る内部ホスト６０１は、セッション管理部６０６、トンネリング処理部６０７を構成要素にもつ。

【００６４】一方、本実施形態に係るファイアウォール６０３の構成要素は、セッション管理部６０８、アクセス制御部６０９の２つである。

【００６５】本実施形態に係る端末６０５の構成要素は、第１の実施形態の場合と同じ、すなわち、セッション管理部６１０、移動前情報記憶部６１１、トンネリング処理部６１２の３つである。ここで、移動前情報記憶部６１１は、端末６０５の移動前アドレスＩ２、内部ホスト６０１のアドレスＩ１を記憶している。

【００６６】なお、本実施形態の場合には、２つのトンネルを用意する。１つは、内部ホスト６０１とファイアウォール６０３の間のトンネル６１３であり、１つは、ファイアウォール６０３と端末６０５の間のトンネル６１４である。

【００６７】内部ホスト６０１は、端末６０５のアドレスとして移動前アドレスＩ２を使用して、パケットをトンネリング処理部６０７と入出力する。

【００６８】端末６０５は、端末６０５のアドレスとして移動前アドレスＩ２を使用して、パケットをトンネリング処理部６１２と入出力する。

【００６９】セッション管理部６０８とセッション管理

部６１０は、互いに通信し、端末６０５の認証と鍵交換をする。ここで、セッション管理部６１０は、セッション管理部６０８へ、端末６０５が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であること、内部ホスト６０１のアドレスがＩ１であることを通知する。一方、セッション管理部６０８は、セッション管理部６０６へ、端末６０５が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であること、及び鍵を通知する。

【００７０】トンネリング処理部６０７は、セッション管理部６０８が交換した鍵を使用して、端末６０５宛てのパケットを暗号処理しカプセル化する。また、トンネリング処理部６０７は、内部ホスト６０１宛てのパケットを脱カプセル化し復号処理する。

【００７１】トンネリング処理部６１２は、セッション管理部６１０が交換した鍵を使用して、内部ホスト６０１宛てのパケットを暗号処理しカプセル化する。また、トンネリング処理部６１２は、端末６０５宛てのパケットを脱カプセル化し復号処理する。

【００７２】アクセス制御部６０９は、受信するパケットが、内部ホスト６０１と端末６０５の間の通信のパケットであるかを判定する。アクセス制御部６０９は、内部ホスト６０１と端末６０５の間の通信のパケットを中継する。アクセス制御部６０９は、内部ホスト６０１と端末６０５の間の通信ではないパケットを中継しない。

【００７３】（Ｃ－２）第２の実施形態の動作

続いて、図６に示す通信システムによって実現される通信動作を説明する。

【００７４】（Ｃ－２－１）通信開始前の動作

まず、内部ホスト６０１と端末６０５が通信を開始するまでの動作を説明する。

【００７５】セッション管理部６０８とセッション管理部６１０が通信し、端末６０５の認証と鍵交換をする。セッション管理部６１０は、セッション管理部６０８へ、端末６０５が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であること、内部ホスト６０１のアドレスがＩ１であることを通知する。セッション管理部６０８は、セッション管理部６０６へ、端末６０５が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であること、及び鍵を通知する。これにより、アクセス制御部６０９は、内部ホスト６０１と端末６０５の間のパケットを中継するようになる。

【００７６】（Ｃ－２－２）通信開始後の動作

次に、内部ホスト６０１と端末６０５が通信する時の動作を説明する。

【００７７】なお、内部ホスト６０１から端末６０５へ伝送されるパケット６１５の受信先アドレスはＩ２、送信元アドレスはＩ１となる。また、このパケット６１５をカプセル化したパケット６１６の受信先アドレスはＥ、送信元アドレスはＩ１となる。なお、パケット６１７は、パケット６１６と同一である。パケット６１８は、パケット６１５と同一である。

【００７８】一方、端末６０５から内部ホスト６０１へ伝送されるパケット６１９の受信先アドレスはＩ１、送信元アドレスはＩ２となる。また、このパケット６１９をカプセル化したパケット６２０の受信先アドレスはＩ１、送信元アドレスはＥとなる。なお、パケット６２１は、パケット６２０と同一である。パケット６２２は、パケット６１９と同一である。

【００７９】（Ｃ－２－２－１）内部ホストから端末への送信

まず、内部ホスト６０１から端末６０５にパケットを送信する場合の動作を説明する。

【００８０】内部ホスト６０１は、パケット６１５をトンネリング処理部６０７へ入力する。トンネリング処理部６０７は、セッション管理部６０８が交換した鍵を使用して、パケット６１５を暗号処理しカプセル化しパケット６１６を得る。この時、パケット６１５の受信先アドレスがＩ２であるので、パケット６１６の受信先アドレスをＥにする。トンネリング処理部６０７は、「通信路Ａ」６０２へパケット６１６を送信する。

【００８１】ファイアウォール６０３のアクセス制御部６０９は、「通信路Ａ」６０２からパケット６１６を受信する。アクセス制御部６０９は、パケット６１６が内部ホスト６０１と端末６０５の間のパケットであると判定する。アクセス制御部６０９は、「通信路Ｂ」６０４へパケット６１７を送信する。トンネリング処理部６１２は、「通信路Ｂ」６０４からパケット６１７を受信する。トンネリング処理部６１２は、セッション管理部６１０が交換した鍵を使用して、パケット６１７を脱カプセル化し復号処理し、パケット６１８を得る。

【００８２】端末６０５は、トンネリング処理部６１２からパケット６１８を得る。

【００８３】（Ｃ－２－２－２）端末から内部ホストへの送信

逆に、端末６０５から内部ホスト６０１にパケットを送信する場合の動作を説明する。

【００８４】端末６０５は、パケット６１９をトンネリング処理部６１２に入力する。トンネリング処理部６１２は、セッション管理部６１０が交換した鍵を使用して、パケット６１９を暗号処理しカプセル化しパケット６２０を得る。この時、パケット６１９の受信先アドレスがＩ１であるので、パケット６２０の受信先アドレスをＩ１にする。

【００８５】ファイアウォール６０３のアクセス制御部６０９は、パケット６２０が内部ホスト６０１と端末６０５の間のパケットであると判定し、パケット６２０を中継する。

15

【００８６】内部ホスト６０１のトンネリング処理部６０７は、セッション管理部６０８が交換した鍵を使用して、パケット６２１を脱カプセル化し復号処理しパケット６２２を得る。

【００８７】（Ｃ－３）第２の実施形態の効果

以上のように、第２の実施形態によれば、内部ホストと端末との間にトンネルを設けるので、内部ネットワークにおいて、受信先アドレスが端末の移動前アドレスＩ２であるパケットがファイアウォールに届かない場合であっても、ルーティングテーブルを変更することなく経路制御をすることができる。これにより、外部ネットワークに移動した端末は任意の内部ホストにアクセスできるようになる。

【００８８】また、第２の実施形態によれば、複数の内部ホスト６０１と複数の端末６０５が同時に通信可能である。

【００８９】（Ｄ）第３の実施形態

続いて、第３の実施形態を説明する。ところで、第２の実施形態では、外部ネットワークにおいて、ヘッダに内部ホストのアドレスを含むパケットを伝送する形態となるため、外部ネットワークにおいて内部ホストのアドレスを隠蔽できない。そこで、次の実施形態を考える。

【００９０】（Ｄ－１）第３の実施形態の構成

図７は、第３の実施形態の構成図である。この通信システムの場合も基本構成は、内部ホスト７０１、「通信路Ａ」７０２、ファイアウォール７０３、「通信路Ｂ」７０４、端末７０５である。なお、図７は、図６との対応部分に対応符号を付して示すもので、セッション管理部７０６～トンネリング処理部７１２は、それぞれ、図６のセッション管理部６０６～トンネリング処理部６１２に対応している。これらの構成は、第２の実施形態の場合と同様である。また、トンネル内のパケットを除く各パケット７１５、７１８、７１９、７２２も、第２の実施形態の場合と同様である。

【００９１】従って、本実施形態と第２の実施形態との違いは、本実施形態に係るファイアウォール７０３がアドレス変換部７２３を構成要素として有している点にある。このアドレス変換部７２３は、ファイアウォール７０３のアクセス制御部７０９が中継するパケットのヘッダアドレスを書き換える役割をもつものである。

【００９２】（Ｄ－２）第３の実施形態の動作

続いて、図７に示す通信システムによって実現される通信動作を説明する。なお、以下の説明では、第３の実施形態の動作のうち、第２の実施形態の動作と異なる動作を重点的に説明することにする。

【００９３】（Ｄ－２－１）通信開始前の動作

まず、内部ホスト７０１と端末７０５が通信を開始するまでの動作であるが、これは、第２の実施形態の場合と同様である。すなわち、セッション管理部７０６と７０８及びセッション管理部７０８と７１０の間で通信がなされ、端末７０５の移動が通知される。

16

【００９４】（Ｄ－２－２）通信開始後の動作

次に、内部ホスト７０１と端末７０５が通信する時の動作を説明する。

【００９５】ただし、この実施形態の場合には、内部ホスト７０１から端末７０５へ伝送されるパケット７１５をカプセル化したパケット７１６の受信先アドレスがＦｉ、送信元アドレスがＩ１となる。しかも、このパケット７１６のアドレスは書き換えの対象となるので、パケット７１７の受信先アドレスはＥ、送信元アドレスはＦｅとなる。その反対に、端末７０５から内部ホスト７０１へ伝送されるパケット７１９をカプセル化したパケット７２０の受信先アドレスはＦｅ、送信元アドレスはＥとなる。また同様に、パケット７２１の受信先アドレスはＩ１、送信元アドレスはＦｉとなる。

【００９６】（Ｄ－２－２－１）内部ホストから端末への送信

まず、内部ホスト７０１から端末７０５にパケットを送信する場合の動作を説明する。

【００９７】アクセス制御部７０９がパケット７１６は内部ホスト７０１と端末７０５の間の通信のパケットであると判定するまでの動作は、第２の実施形態の場合と同様である。

【００９８】アクセス制御部７０９は、パケット７１６をアドレス変換部７２３に入力する。アドレス変換部７２３は、パケット７１６のヘッダのアドレスを書き換え、パケット７１７を得る。この時、パケット７１６の送信元アドレスがＩ１であるので、パケット７１７の受信先アドレスをＥにする。アドレス変換部７２３は、アクセス制御部７０９へパケット７１７を出力する。

【００９９】端末７０５がパケット７１８を得るまでの動作は、第２の実施形態と同様である。

【０１００】（Ｄ－２－２－２）端末から内部ホストへの送信

逆に、端末７０５から内部ホスト７０１にパケットを送信する場合の動作を説明する。

【０１０１】アクセス制御部７０９がパケット７２０が内部ホスト７０１と端末７０５の間の通信のパケットであると判定するまでの動作は、第２の実施形態と同様である。

【０１０２】アクセス制御部７０９は、パケット７２０をアドレス変換部７２３に入力する。アドレス変換部７２３は、パケット７２０のヘッダのアドレスを書き換え、パケット７２１を得る。この時、パケット７２０の送信元アドレスがＥであるので、パケット７２１の受信先アドレスをＩ１にする。

【０１０３】アドレス変換部７２３は、アクセス制御部７０９にパケット７２１を出力する。内部ホスト７０１がパケット７２２を得るまでの動作は、第２の実施形態と同様である。

【０１０４】（Ｄ－３）第３の実施形態の効果
以上のように、第３の実施形態によれば、ファイアウォールにアドレスを変換する機能を備えたので、外部ネットワークに、内部ホストのアドレスを隠蔽できるという効果が得られる。
【０１０５】（Ｅ）第４の実施形態
続いて、第４の実施形態を説明する。ところで、第３の実施形態では、内部ホスト７０１から端末７０５へパケットを送信する場合に、パケット７１６の送信元アドレス１１により、パケット７１７の受信先アドレスＥを決定する。また、端末７０５から内部ホスト７０１へパケットを送信する場合に、パケット７２０の送信元アドレスＥにより、パケット７２１の受信先アドレスＩ１を決定する。従って、外部ネットワークに移動した端末７０５が、ある内部ホスト７０１と通信中の場合には、外部ネットワークに移動した他の端末７０５は、同じ内部ホスト７０１と同時に通信を行うことができない。そこで、次の構成を考える。
【０１０６】（Ｅ－１）第４の実施形態の構成
図８は、第４の実施形態の構成図である。この通信システムの場合も基本構成は、内部ホスト８０１、「通信路Ａ」８０２、ファイアウォール８０３、「通信路Ｂ」８０４、端末８０５である。また、図７との対応部分に対応符号を付して示した図８から分かるように、これらを構成する各構成要素も基本的には、第３の実施形態と同じである。
【０１０７】本実施形態が第３の実施形態と異なっているのは、ファイアウォール８０３が、外部ネットワークに接続しているネットワーク・インターフェースのアドレスと内部ネットワークに接続しているネットワーク・インターフェースのアドレスをそれぞれ複数有する点である。すなわち、ファイアウォール８０３は、外部ネットワークに接続しているネットワーク・インターフェースのアドレスとしてＦｅ１～Ｆｅｎ（ｎ＞１）を有し、内部ネットワークに接続しているネットワーク・インターフェースのアドレスとしてＦｉ１～Ｆｉｍ（ｍ＞１）を有する点である。
【０１０８】この点について生じる違いを説明する。セッション管理部８０８とセッション管理部８１０は、互いに通信し、端末８０５の認証と鍵交換をする。ここで、セッション管理部８１０は、セッション管理部８０８へ、端末８０５が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であること、内部ホスト８０１のアドレスがＩ１であることを通知する。
【０１０９】セッション管理部８０８は、複数のアドレスＦｅ１～Ｆｅｎのうち、その時点で使用していないアドレスＦｅｉを求める。セッション管理部８０８は、Ｆｉ１～Ｆｉｍのうち、その時点で使用していないアドレスＦｉｊを求める。セッション管理部８０８は、セッション管理部８１０に、内部ホスト８０１と端末８０５の通信で使用するファイアウォール８０３の外部アドレスがＦｅｉであることを通知する。
【０１１０】セッション管理部８０８は、セッション管理部８０６へ、端末８０５が外部ネットワークへ移動したこと、移動前アドレスがＩ２であること、内部ホスト８０１と端末８０５の通信で使用するファイアウォール８０３の内部アドレスがＦｉｊであること、鍵を通知する。
【０１１１】（Ｅ－２）第４の実施形態の動作
続いて、図８に示す通信システムによって実現される通信動作を説明する。なお、以下の説明では、第４の実施形態の動作のうち、第３の実施形態の動作と異なる動作を重点的に説明することにする。
【０１１２】（Ｅ－２－１）通信開始前の動作
まず、内部ホスト８０１と端末８０５が通信を開始するまでの動作を説明する。
【０１１３】セッション管理部８０８とセッション管理部８１０は、互いに通信し、端末８０５の認証と鍵交換をする。セッション管理部８１０は、セッション管理部８０８へ、端末８０５が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であること、内部ホスト８０１のアドレスがＩ１であることを通知する。
【０１１４】セッション管理部８０８は、複数有するＦｅ１～Ｆｅｎのうち、その時点で使用していないアドレスＦｅｉを求める。セッション管理部８０８は、Ｆｉ１～Ｆｉｍのうち、その時点で使用していないアドレスＦｉｊ求める。
【０１１５】セッション管理部８０８は、セッション管理部８１０へ、内部ホスト８０１と端末８０５の通信で使用するファイアウォール８０３の外部アドレスがＦｅｉであることを通知する。また、セッション管理部８０８は、セッション管理部８０６へ、端末８０５が外部ネットワークへ移動したこと、移動前アドレスがＩ２であること、内部ホスト８０１と端末８０５の通信で使用するファイアウォール８０３の内部アドレスがＦｉｊであること、鍵を通知する。
【０１１６】（Ｅ－２－２）通信開始後の動作
次に、内部ホスト８０１と端末８０５が通信する場合の動作を説明する。なおここでは、第４の実施形態の動作のうち、第２の実施形態の動作とは異なる動作を説明する。
【０１１７】なお、内部ホスト８０１から端末８０５へ伝送されるパケット８１５の受信先アドレスはＩ２、送信元アドレスはＩ１となる。また、このパケット８１５をカプセル化したパケット８１６の受信先アドレスはＦｉｊ、送信元アドレスはＩ１となる。なお、パケット８１７は、パケット８１６のヘッダのアドレスを書き換えたパケットであり、その受信先アドレスはＥ、送信元ア

ドレスはＦｅｉである。パケット８１８は、パケット８１５と同一である。

【０１１８】一方、端末８０５から内部ホスト８０１へ伝送されるパケット８１９の受信先アドレスはＩ１、送信元アドレスはＩ２となる。また、このパケット８１９をカプセル化したパケット８２０の受信先アドレスはＦｅｉ、送信元アドレスはＥとなる。パケット８２１は、パケット８２０のヘッダのアドレスを書き換えたパケットであり、その受信先アドレスはＩ１、送信元アドレスはＦｉｊとなる。パケット８２２は、パケット８１９と同一である。

【０１１９】（Ｅ－２－２－１）内部ホストから端末への送信

まず、内部ホスト８０１から端末８０５にパケットを送信する場合の動作を説明する。

【０１２０】トンネリング処理部８０７は、パケット８１５の受信先アドレスがＩ２であるので、パケット８１６の受信先アドレスをＦｉｊにする。

【０１２１】ファイアウォール８０３のアドレス変換部８２３は、パケット８１６の受信先アドレスがＦｉｊであるので、パケット８１７の受信先アドレスをＥにする。

【０１２２】（Ｅ－２－２－２）端末から内部ホストへの送信

逆に、端末８０５から内部ホスト８０１にパケットを送信する場合の動作を説明する。

【０１２３】トンネリング処理部８１２は、パケット８１９の受信先アドレスがＩ１であるので、パケット８２０の受信先アドレスをＦｅｉにする。

【０１２４】ファイアウォール８０３のアドレス変換部８２３は、パケット８２０の受信先アドレスがＦｅｉであるので、パケット８２１の受信先アドレスをＩ１にする。

【０１２５】（Ｅ－３）第４の実施形態の効果

以上のように、第４の実施形態によれば、ファイアウォールの外部アドレスと内部アドレスを複数にしたので、複数の内部ホストと複数の端末が同時に通信可能となる効果が得られる。

【０１２６】（Ｆ）第５の実施形態

続いて、第５の実施形態を説明する。ところで、第４の実施形態では、ファイアウォールに複数の外部アドレスと複数の内部アドレスを割り当てる必要がある。そこで、次の構成を考える。

【０１２７】（Ｆ－１）第５の実施形態の構成

従来技術に示した文献においては、カプセル化した後のパケットのヘッダには、受信先アドレスと送信元アドレス以外に、ＳＰＩ（Security Parameters Index）を含む。ＳＰＩにより、使用する暗号アルゴリズムや鍵などのセキュリティに関係するパラメータを表している。パケットを受信するコンピュータは、ＳＰＩを決めて、パケットを送信するコンピュータに、ＳＰＩを通知する。

【０１２８】そこで、第５の実施形態においては、パケットがどの内部ホストとどの端末の間の通信のパケットであるかを、ＳＰＩにより表すことにする。

【０１２９】図９は、第５の実施形態の構成図である。図９は、第３の実施形態の説明に用いた図７との対応部分に対応符号を付したものである。従って、ここでは、本実施形態の構成のうち、第３の実施形態の構成と異なる部分を説明する。

【０１３０】セッション管理部９０８とセッション管理部９１０は、互いに通信し、端末９０５の認証と鍵交換をする。

【０１３１】セッション管理部９１０は、内部ホスト９０１が端末９０５へ送信するパケットのＳＰＩ（ここではＢとする。）を求める。セッション管理部９１０は、セッション管理部９０８へ、端末９０５が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であること、内部ホスト９０１のアドレスがＩ１であること、内部ホスト９０１が端末９０５へ送信するパケットのＳＰＩがＢであることを通知する。

【０１３２】セッション管理部９０８は、セッション管理部９０６へ、端末９０５が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であること、内部ホスト９０１が端末９０５へ送信するパケットのＳＰＩがＢであること、鍵を通知する。

【０１３３】セッション管理部９０６は、端末９０５が内部ホスト９０１へ送信するパケットのＳＰＩ（ここでは、Ａとする。）を求める。セッション管理部９０６は、セッション管理部９０８へ、端末９０５が内部ホスト９０１へ送信するパケットのＳＰＩがＡであることを通知する。セッション管理部９０８は、セッション管理部９１０へ、端末９０５が内部ホスト９０１へ送信するパケットのＳＰＩがＡであることを通知する。

【０１３４】トンネリング処理部９０７は、パケット９１５をカプセル化する時に、ＳＰＩをＢにする。トンネリング処理部９１２は、パケット９１９をカプセル化する時に、ＳＰＩをＡにする。

【０１３５】アドレス変換部９２３は、ＳＰＩにより、パケットのヘッダのアドレスを書き換える。

【０１３６】（Ｆ－２）第５の実施形態の動作

続いて、図９に示す通信システムによって実現される通信動作を説明する。

【０１３７】（Ｆ－２－１）通信開始前の動作

まず、内部ホスト９０１と端末９０５が通信を開始するまでの動作を説明する。

【０１３８】セッション管理部９０８とセッション管理部９１０は、互いに通信し、端末９０５の認証と鍵交換をする。

【０１３９】セッション管理部９１０は、内部ホスト９０１が端末９０５へ送信するパケットのＳＰＩ（ここではＢとする。）を求める。セッション管理部９１０は、セッション管理部９０８へ、端末９０５が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であること、内部ホスト９０１のアドレスがＩ１であること、内部ホスト９０１が端末９０５へ送信するパケットのＳＰＩがＢであることを通知する。

【０１４０】セッション管理部９０８は、セッション管理部９０６へ、端末９０５が外部ネットワークへ移動したこと、移動前アドレスがＩ２であること、内部ホスト９０１が端末９０５へ送信するパケットのＳＰＩがＢであること、鍵を通知する。

【０１４１】セッション管理部９０６は、端末９０５が内部ホスト９０１へ送信するパケットのＳＰＩ（ここでは、Ａとする。）を求める。セッション管理部９０６は、セッション管理部９０８へ、端末９０５が内部ホスト９０１へ送信するパケットのＳＰＩがＡであることを通知する。

【０１４２】セッション管理部９０８は、セッション管理部９１０へ、端末９０５が内部ホスト９０１へ送信するパケットのＳＰＩがＡであることを通知する。

【０１４３】（Ｆ－２－２）通信開始後の動作

次に、内部ホスト９０１と端末９０５が送信する場合の動作を説明する。なおここでは、第５の実施形態の動作のうち、第３の実施形態の動作とは異なる動作を説明する。

【０１４４】なお、内部ホスト９０１から端末９０５へ伝送されるパケット９１５の受信先アドレスはＩ２、送信元アドレスはＩ１となる。また、このパケット９１５をカプセル化したパケット９１６の受信先アドレスはＦｉ、送信元アドレスはＩ１、ＳＰＩはＢである。パケット９１７は、パケット９１６のヘッダのアドレスを書き換えたパケットであり、受信先アドレスはＥ、送信元アドレスはＦｅ、ＳＰＩはＢである。パケット９１８は、パケット９１５と同一である。

【０１４５】一方、端末９０５から内部ホスト９０１へ伝送されるパケット９１９の受信先アドレスはＩ１、送信元アドレスはＩ２となる。パケット９２０は、このパケット９１９をカプセル化したパケットであり、その受信先アドレスはＦｅ、送信元アドレスはＥ、ＳＰＩはＡとなる。パケット９２１は、パケット９２０のヘッダのアドレスを書き換えたパケットであり、受信先アドレスはＩ１、送信元アドレスはＦｉ、ＳＰＩはＡである。パケット９２２は、パケット９１９と同一である。

【０１４６】（Ｆ－２－２－１）内部ホストから端末への送信

内部ホスト９０１から端末９０５にパケットを送信する場合の動作を説明する。

【０１４７】内部ホスト９０１は、パケット９１５をトンネリング処理部９０７に入力する。トンネリング処理部９０７は、パケット９１５を暗号処理しカプセル化しパケット９１６を得る。この時、パケット９１５の受信先アドレスがＩ２であるので、パケット９１６のＳＰＩをＢとする。トンネリング処理部９０７はパケット９１６を「通信路Ａ」９０２に送信する。

【０１４８】ファイアウォール９０３のアクセス制御部９０９は、「通信路Ａ」９０２からパケット９１６を受信する。アクセス制御部９０９は、パケット９１６をアドレス変換部９２３に入力する。アドレス変換部９２３は、パケット９１６のヘッダのアドレスを書き換え、パケット９１７を得る。この時、パケット９１６のＳＰＩがＢであることから、パケット９１７の受信先アドレスをＥとする。

【０１４９】端末９０５がパケット９１８を得るまでの動作は、第３の実施形態と同様である。

【０１５０】（Ｆ－２－２－２）端末から内部ホストへの送信

逆に、端末９０５から内部ホスト９０１にパケットを送信する場合の動作を説明する。

【０１５１】端末９０５は、パケット９１９をトンネリング処理部９１２へ入力する。トンネリング処理部９１２は、パケット９１９を暗号処理しカプセル化しパケット９２０を得る。この時、パケット９１９の受信先アドレスがＩ１であるので、パケット９２０のＳＰＩをＡとする。トンネリング処理部９１２は、「通信路Ｂ」９０４にパケット９２０を送信する。

【０１５２】ファイアウォール９０３のアクセス制御部９０９は、「通信路Ｂ」９０４からパケット９２０を受信する。アクセス制御部９０９は、パケット９２０をアドレス変換部９２３に入力する。アドレス変換部９２３は、パケット９２０のヘッダのアドレスを書き換えパケット９２１を得る。この時、パケット９２０のＳＰＩがＡであることから、パケット９２１の受信先アドレスをＩ１とする。

【０１５３】内部ホスト９０１がパケット９２２を得るまでの動作は、実施形態３の動作と同様である。

【０１５４】（Ｆ－３）第５の実施形態の効果

以上のように、第５の実施形態によれば、パケットヘッダに書き込まれているＳＰＩにより、パケットがどの内部ホストとどの端末の間の通信のパケットであるかを表すようにしたので、ファイアウォールに複数の外部アドレスと複数の内部アドレスを割り当てなくても、複数の内部ホストと複数の端末が同時に通信可能となる効果が得られる。

【０１５５】（Ｇ）第６の実施形態

続いて、第６の実施形態を説明する。ところで、第２、第３、第４、第５の実施形態では、内部ネットワークのあるサブネットに位置する端末を、内部ネットワークの

他のサブネットへ移動すると、端末のアドレスが変化するので、端末は移動前のサービス利用権限で内部ホストが提供するサービスを利用できなくなることがある。そこで、次の構成を考える。

【０１５６】なお、第６の実施形態では、端末が外部ネットワークに移動する場合に係る構成と動作は、第２の実施形態と同様である。以下では、第６の実施形態の構成と動作のうち、第２の実施形態の構成と動作とは異なる構成と動作を説明する。

【０１５７】（Ｇ－１）第６の実施形態の構成

図１０は、第６の実施形態の構成図である。図１０には、内部ネットワークのあるサブネットに位置する端末を、内部ネットワークの他のサブネット（サブネットＡ）へ移動する場合に係る構成要素のみを示してある。また、図１０は、端末を外部ネットワークへ移動する場合に係る構成要素の一部を示したものである。従って、図１０では、内部ホスト１００１、「通信路Ｃ」１００２、端末１００３の３つのみを示している。

【０１５８】本実施形態に係る内部ホスト１００１は、外部セッション管理部１００４、内部セッション管理部１００５、トンネリング処理部１００６を構成要素としてもつ。

【０１５９】本実施形態に係る端末１００３は、内部セッション管理部１００７、外部セッション管理部１００８、移動前情報記憶部１００９、トンネリング処理部１０１０を構成要素としてもつ。

【０１６０】また、内部ホスト１００１と端末１００３の間にトンネル１０１１を設ける。

【０１６１】ここで、「通信路Ｃ」１００２は、内部ホスト１００１と端末１００３の間の通信路である。すなわち、「通信路Ｃ」１００２は、内部ネットワークの通信路である。

【０１６２】また、第２の実施形態と同様、ファイアウォールの構成要素は、セッション管理部とアクセス制御部である。内部ホスト１００１とファイアウォールとの間には、「通信路Ａ」とトンネルがある。ファイアウォールと外部ネットワークに移動した端末との間には、「通信路Ｂ」とトンネルがある。

【０１６３】外部セッション管理部１００８とファイアウォールのセッション管理部は、互いに通信し、外部ネットワークに移動した端末の認証と鍵交換をする。外部セッション管理部１００８は、ファイアウォールのセッション管理部へ、端末が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であること、内部ホスト１００１のアドレスがＩ１であることを、通知する。

【０１６４】ファイアウォールのセッション管理部は、外部セッション管理部１００４へ、端末が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であること、鍵を通知する。

【０１６５】内部セッション管理部１００５と内部セッション管理部１００７は、互いに通信し、端末１００３の認証と鍵交換をする。内部セッション管理部１００７は、内部セッション管理部１００５へ、端末１００３が内部ネットワークの他のサブネットに移動したこと、移動後のアドレスがＩ２’であること、移動前アドレスがＩ２であることを通知する。

【０１６６】トンネリング処理部１００６は、内部セッション管理部１００５が交換した鍵を使用して、端末１００３宛てのパケットを暗号処理してカプセル化する。

【０１６７】また、トンネリング処理部１００６は、外部セッション管理部１００４が交換した鍵を使用して、外部ネットワークへ移動した端末宛てのパケットを暗号処理してカプセル化する。トンネリング処理部１００６は、内部ホスト１００１宛てのパケットを脱カプセル化し復号処理する。

【０１６８】トンネリング処理部１０１０は、内部セッション管理部１００７が交換した鍵を使用して、内部ホスト１００１宛てのパケットを暗号処理しカプセル化する。また、トンネリング処理部１０１０は、外部セッション管理部１００８が交換した鍵を使用して、内部ホスト１００１宛てのパケットを暗号処理しカプセル化する。トンネリング処理部１０１０は、端末１００３宛てのパケットを脱カプセル化し復号処理する。

【０１６９】（Ｇ－２）第６の実施形態の動作

続いて、図１０に示す通信システムによって実現される通信動作を説明する。

【０１７０】（Ｇ－２－１）通信開始前の動作

まず、内部ホスト１００１と端末１００３の通信の開始における動作を説明する。

【０１７１】内部セッション管理部１００５と内部セッション管理部１００７は、互いに通信し、端末１００３の認証と鍵交換をする。

【０１７２】内部セッション管理部１００７は、内部セッション管理部１００５に、端末１００３が内部ネットワークの他のサブネットに移動したこと、移動後のアドレスがＩ２’であること、移動前アドレスがＩ２であることを通知する。

【０１７３】（Ｇ－２－２）通信開始後の動作

次に、内部ホスト１００１と端末１００３が通信をする時の動作を説明する。

【０１７４】なお、内部ホスト１００１から端末１００３へ伝送されるパケット１０１２の受信先アドレスはＩ２、送信元アドレスはＩ１となる。また、このパケット１００１２をカプセル化したパケット１０１３の受信先アドレスはＩ２’、送信元アドレスはＩ１である。パケット１０１４は、パケット１０１２と同一である。

【０１７５】一方、端末１００３から内部ホスト１００１へ伝送されるパケット１０１５の受信先アドレスはＩ１、送信元アドレスはＩ２となる。パケット１０１６

は、このパケット１０１５をカプセル化したパケットであり、その受信先アドレスはＩ１、送信元アドレスはＩ２’となる。パケット１０１７は、パケット１０１５と同一である。

【０１７６】（Ｇ－２－２－１）内部ホストから端末への送信

まず、内部ホスト１００１から端末１００３へパケットを送信する場合の動作を説明する。

【０１７７】内部ホスト１００１は、トンネリング処理部１００６にパケット１０１２を入力する。トンネリング処理部１００６は、パケット１０１２を暗号処理しカプセル化しパケット１０１３を得る。この時、パケット１０１２の受信先アドレスがＩ２であるので、パケット１０１３の受信先アドレスを１２’にする。トンネリング処理部１００６は、「通信路Ｃ」１００２にパケット１０１３を送信する。トンネリング処理部１０１０は、「通信路Ｃ」１００２からパケット１０１３を受信する。

【０１７８】トンネリング処理部１０１０は、パケット１０１３を脱カプセル化し復号処理しパケット１０１４を得る。

【０１７９】（Ｇ－２－２－２）端末から内部ホストへの送信

逆に、端末１００３から内部ホスト１００１へパケットを送信する場合の動作を説明する。

【０１８０】端末１００３は、トンネリング処理部１０１０にパケット１０１５を入力する。トンネリング処理部１０１０は、パケット１０１５を暗号処理しカプセル化しパケット１０１６を得る。この時、パケット１０１５の受信先アドレスがＩ１であるので、パケット１０１６の受信先アドレスをＩ１とする。トンネリング処理部１０１０は、「通信路Ｃ」１００２にパケット１０１６を送信する。トンネリング処理部１００６は、「通信路Ｃ」１００２からパケット１０１６を受信する。トンネリング処理部１００６は、パケット１０１６を脱カプセル化し復号処理しパケット１０１７を得る。

【０１８１】内部ホスト１００１は、パケット１０１７を得る。

【０１８２】（Ｇ－３）第６の実施形態の効果

以上のように、第６の実施形態によれば、内部ネットワークの他のサブネットへ移動した端末と内部ホストの間にトンネルを設けるので、端末を内部ネットワークの他のサブネットへ移動しても、端末は移動前のサービス利用権限で内部ホストが提供するサービスを利用できるという効果が得られる。

【０１８３】勿論、第６の実施形態では、複数の内部ホストと複数の端末が同時に通信可能である。

【０１８４】（Ｈ）第７の実施形態

続いて、第７の実施形態を説明する。ところで、第２、第３、第４、第５、第６の実施形態では、内部ホストごとに、端末までトンネルを設ける機能を備える必要がある。そこで、次の構成を考える。

【０１８５】（Ｈ－１）第７の実施形態の構成

図１１は、第７の実施形態の構成図である。本実施形態に係る通信システムは、内部ホスト１１０１、「通信路Ａ」１１０２、サブネット管理サーバ１１０３、「通信路Ｂ」１１０４、ファイアウォール１１０５、「通信路Ｃ」１１０６、端末１１０７からなる。

【０１８６】本実施形態に係るサブネット管理サーバ１１０３は、セッション管理部１１０８、トンネリング処理部１１０９を構成要素とする。

【０１８７】本実施形態に係るファイアウォール１１０５は、セッション管理部１１１０、アクセス制御部１１１１を構成要素とする。

【０１８８】本実施形態に係る端末１１０７は、セッション管理部１１１２、移動前情報記憶部１１１３、トンネリング処理部１１１４を構成要素とする。

【０１８９】「通信路Ａ」１１０２は、内部ホスト１１０１とサブネット管理サーバ１１０３の間の通信路である。すなわち、「通信路Ａ」１１０２は、内部ネットワークの通信路である。「通信路Ｂ」１１０４は、サブネット管理サーバ１１０３とファイアウォール１１０５の間の通信路である。すなわち、「通信路Ｂ」１１０４は、内部ネットワークの通信路である。「通信路Ｃ」１１０６は、ファイアウォール１１０５と端末１１０７の間の通信路である。すなわち、「通信路Ｃ」１１０６は、外部ネットワークの通信路である。

【０１９０】サブネット管理サーバ１１０３とファイアウォール１１０５の間にはトンネル１１１５を設ける。ファイアウォール１１０５と端末１１０７の間にはトンネル１１１６を設ける。

【０１９１】サブネット管理サーバ１１０３は、サブネットごとに設ける。サブネット管理サーバ１１０３が位置するサブネットは、サブネットＡである。なお、端末１１０７は、外部ネットワークへ移動する前にはサブネットＡに位置していたものとする。

【０１９２】端末１１０７が外部ネットワークへ移動した後で内部ホスト１１０１と通信する場合に、サブネット管理サーバ１１０３と端末１１０７の間のトンネルを抜ける。

【０１９３】サブネット管理サーバ１１０３は、内部ホスト１１０１から端末１１０７宛てのパケットを受信し、そのパケットを暗号処理しカプセル化して、トンネルを通して端末１１０７へ送信する。また、サブネット管理サーバ１１０３は、トンネルを通して端末１１０７から内部ホスト１１０１宛てのパケットを受信し、そのパケットを脱カプセル化し復号処理して、内部ホスト１１０１へ送信する。サブネット管理サーバ１１０３のアドレスは、Ｓである。

【０１９４】内部ホスト１１０１は、端末１１０７のア

ドレスとして移動前アドレスＩ２を使用して、パケットを「通信路Ａ」１１０２と送受信する。端末１１０７は、端末１１０７のアドレスとして移動前アドレスＩ２を使用して、パケットをトンネリング処理部１１１４と入出力する。

【０１９５】セッション管理部１１１０とセッション管理部１１１２は、互いに通信し、端末１１０７の認証と鍵交換をする。セッション管理部１１１２は、セッション管理部１１１０へ、端末１１０７が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であること、サブネット管理サーバ１１０３のアドレスがＳであることを通知する。セッション管理部１１１０は、セッション管理部１１０８へ、端末１１０７が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であること、鍵を通知する。

【０１９６】トンネリング処理部１１０９は、セッション管理部１１１０が交換した鍵を使用して、端末１１０７宛てのパケットを暗号処理してカプセル化する。また、トンネリング処理部１１０９は、内部ホスト１１０１宛てのパケットを脱カプセル化し復号処理する。

【０１９７】トンネリング処理部１１１４は、セッション管理部１１１２が交換した鍵を使用して、内部ホスト１１０１宛てのパケットを暗号処理してカプセル化する。

【０１９８】また、トンネリング処理部１１１４は、端末１１０７宛てのパケットを脱カプセル化し復号処理する。

【０１９９】移動前情報記憶部１１１３は、端末１１０７の移動前アドレスＩ２と、サブネット管理サーバ１１０３のアドレスＳを、記憶する。

【０２００】アクセス制御部１１１１は、受信するパケットが、サブネット管理サーバ１１０３と端末１１０７の間の通信のパケットであるかを判定する。アクセス制御部１１１１は、サブネット管理サーバ１１０３と端末１１０７の間の通信のパケットを、中継する。アクセス制御部１１１１は、サブネット管理サーバ１１０３と端末１１０７の間の通信ではないパケットを、中継しない。

【０２０１】（Ｈ－２）第７の実施形態の動作

続いて、図１１に示す通信システムによって実現される通信動作を説明する。

【０２０２】（Ｈ－２－１）通信開始前の動作

まず、内部ホスト１１０１と端末１１０７が通信を開始するまでの動作を説明する。

【０２０３】セッション管理部１１１０とセッション管理部１１１２が通信し、端末１１０７の認証と鍵交換をする。セッション管理部１１１２は、セッション管理部１１１０へ、端末１１０７が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であること、サブネット管理サーバ１１０３のアドレスがＳであることを通知する。セッション管理部１１１０は、セッション管理部１１０８へ、端末１１０７が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であること、鍵を通知する。

【０２０４】（Ｈ－２－２）通信開始後の動作

次に、内部ホスト１１０１と端末１１０７が、通信をする時の動作を説明する。なお、内部ホスト１１０１から端末１１０７へ伝送されるパケット１１１７の受信先アドレスはＩ２、送信元アドレスはＩ１となる。また、パケット１１１８は、このパケット１１１７をカプセル化したパケットであり、その受信先アドレスはＥ、送信元アドレスはＳとなる。パケット１１１９は、パケット１１１８と同一である。パケット１１２０は、パケット１１１７と同一である。

【０２０５】一方、端末１１０７から内部ホスト１１０１へ伝送されるパケット１１２１の受信先アドレスはＩ１、送信元アドレスはＩ２となる。パケット１１２２は、このパケット１１２１をカプセル化したパケットであり、その受信先アドレスはＳ、送信元アドレスはＥとなる。パケット１１２３は、パケット１１２２と同一である。パケット１１２４は、パケット１１２１と同一である。

【０２０６】（Ｈ－２－２－１）内部ホストから端末への送信

まず、内部ホスト１１０１から端末１１０７にパケットを送信する場合の動作を説明する。

【０２０７】内部ホスト１１０１は、「通信路Ａ」１１０２にパケット１１１７を送信する。

【０２０８】サブネット管理サーバ１１０３のトンネリング処理部１１０９は、「通信路Ａ」１１０２からパケット１１１７を受信する。トンネリング処理部１１０９は、パケット１１１７を暗号処理しカプセル化しパケット１１１８を得る。この時、パケット１１１７の受信先アドレスがＩ２であるので、パケット１１１８の受信先アドレスをＥにする。トンネリング処理部１１０９は、パケット１１１８を「通信路Ｂ」１１０４に送信する。アクセス制御部１１１１は、「通信路Ｂ」１１０４からパケット１１１８を受信する。

【０２０９】ファイアウォール１１０５のアクセス制御部１１１１は、パケット１１１８がサブネット管理サーバ１１０３と端末１１０７の間の通信のパケットであると判定する。アクセス制御部１１１１は、パケット１１１８を「通信路Ｃ」１１０６へ送信する。

【０２１０】端末１１０７がパケット１１２０を得るまでの動作は、実施形態２の動作と同様である。

【０２１１】（Ｈ－２－２－２）端末から内部ホストへの送信

逆に、端末１１０７から内部ホスト１１０１にパケット

を送信する場合の動作を説明する。

【０２１２】端末１１０７は、パケット１１２１をトンネリング処理部１１１４へ入力する。トンネリング処理部１１１４は、パケット１１２１を暗号処理しカプセル化しパケット１１２２を得る。この時、サブネット管理サーバ１１０３のアドレスがＳであるので、パケット１１２２の受信先アドレスをＳにする。トンネリング処理部１１１４は、パケット１１２２を「通信路Ｃ」１１０６へ送信する。アクセス制御部１１１１は、「通信路Ｃ」１１０６からパケット１１２２を受信する。ファイアウォール１１０５のアクセス制御部１１１１は、パケット１１２２がサブネット管理サーバ１１０３と端末１１０７の間の通信のパケットであると判定する。アクセス制御部１１１１は、パケット１１２２を「通信路Ｂ」１１０４へ送信する。

【０２１３】サブネット管理サーバ１１０３のトンネリング処理部１１０９は、「通信路Ｂ」１１０４からパケット１１２３を受信する。トンネリング処理部１１０９は、パケット１１２３を脱カプセル化し復号処理し、パケット１１２４を得る。トンネリング処理部１１０９は、「通信路Ａ」１１０２へパケット１１２４を送信する。

【０２１４】内部ホスト１１０１は、パケット１１２４を受信する。

【０２１５】（Ｈ－３）第７の実施形態の効果

以上のように、第７の実施形態によれば、端末との間にトンネルを設けるコンピュータ（サブネット管理サーバ）をサブネットごとに設けるので、内部ホストごとに、端末までトンネルを設ける機能を備える必要がなくなるという効果が得られる。

【０２１６】また、第７の実施形態では、あるサブネット管理サーバ１１０３と複数の端末１１０７が同時に通信可能である。また、複数の内部ホスト１１０１と複数の端末１１０７が同時に通信可能である。

【０２１７】さらに、移動前情報記憶部１１１３がサブネット管理サーバ１１０３のアドレスＳを記憶することと、セッション管理部１１１２がセッション管理部１１１０にサブネット管理サーバ１１０３のアドレスがＳであることを通知することの代わりに、セッション管理部１１１０が、端末１１０７の移動前アドレスからサブネット管理サーバ１１０３のアドレスを求める方式も実施可能である。

【０２１８】（Ｉ）第８の実施形態

続いて、第８の実施形態を説明する。ところで、第７の実施形態では、外部ネットワークで、ヘッダにサブネット管理サーバのアドレスを含むパケットを伝送しているため、外部ネットワークに、サブネット管理サーバのアドレスを隠蔽できない。そこで、次の構成を考える。

【０２１９】（Ｉ－１）第８の実施形態の構成

図１２は、第８の実施形態の構成図である。図１２は、図１１との対応部分に対応符号を付して示したものである。従って、内部ホスト１２０１～トンネル１２１６までの構成は、図１１の内部ホスト１１０１～トンネル１１１６までと同様である。また、パケットのうち、１２１７、１２２０、１２２１、１２２４は、それぞれ、図１１のパケット、１１１７、１１２０、１１２１、１１２４と同様である。

【０２２０】相違点は、ファイアウォール１２０５にアドレス変換部１２２５が設けられている点である。このアドレス変換部１２２５は、ファイアウォール１２０５のアクセス制御部１２１１が中継するパケットのヘッダのアドレスを書き換える。

【０２２１】（Ｉ－２）第８の実施形態の動作

ここでは、第８の実施形態の動作のうち、第７の実施形態の動作とは異なる動作を説明する。

【０２２２】（Ｉ－２－１）通信開始前の動作

まず、内部ホスト１２０１と端末１２０７が通信を開始するまでの動作を説明する。

【０２２３】この場合も、各セッション管理部１２０８、１２１０、１２１２が通信し、認証と鍵交換、また、移動情報やアドレスを確認し合う。

【０２２４】パケット１２１８は、内部ホスト１２０１から端末１２０７へ送信されるパケット１２１７をカプセル化したパケットであり、その受信先アドレスはＦｉ、送信元アドレスはＳとなる。パケット１２１９は、このパケット１２１８のヘッダのアドレスを書き換えたパケットであり、その受信先アドレスはＥ、送信元アドレスはＦｅとなる。

【０２２５】一方、パケット１２２２は、端末１２０７から内部ホスト１２０１へ送信されるパケット１２２１をカプセル化したパケットであり、その受信先アドレスはＦｅ、送信元アドレスはＥとなる。パケット１２２３は、このパケット１２２２のヘッダアドレスを書き換えたパケットであり、その受信先アドレスはＳ、送信元アドレスはＦｉとなる。

【０２２６】（Ｉ－２－２）通信開始後の動作

（Ｉ－２－２－１）内部ホストから端末への送信

まず、内部ホスト１２０１から端末１２０７にパケットを送信する場合の動作を説明する。

【０２２７】アクセス制御部１２１１は、パケット１２１８をアドレス変換部１２２５に入力する。アドレス変換部１２２５は、パケット１２１８のヘッダのアドレスを書き換えパケット１２１９を得る。この時、パケット１２１８の送信元アドレスがＳであるので、パケット１２１９の受信先アドレスをＥにする。

【０２２８】アドレス変換部１２２５は、パケット１２１９をアクセス制御部１２１１へ出力する。

【０２２９】（Ｉ－２－２－２）端末から内部ホストへの送信

逆に、端末１２０７から内部ホスト１２０１にパケット

を送信する場合の動作を説明する。

【０２３０】アクセス制御部１２１１は、パケット１２２２をアドレス変換部１２２５に入力する。アドレス変換部１２２５は、パケット１２２２のヘッダのアドレスを書き換え、パケット１２２３を得る。この時、パケット１２２２の送信元アドレスがＥであるので、パケット１２２３の受信先アドレスをＳにする。

【０２３１】アドレス変換部１２２５は、パケット１２２３をアクセス制御部１２１１に出力する。

【０２３２】（Ｉ－３）第８の実施形態の効果

以上のように、第８の実施形態によれば、ファイアウォールにアドレスを変換する機能を備えたので、外部ネットワークに、サブネット管理サーバのアドレスを隠蔽できるという効果が得られる。

【０２３３】（Ｊ）第９の実施形態

続いて、第９の実施形態を説明する。ところで、第８の実施形態では、あるサブネット管理サーバ１２０３とは同時に一つの端末しか通信できない。そこで、次の構成を考える。

【０２３４】（Ｊ－１）第９の実施形態の構成

図１３は、第９の実施形態の構成図である。図１３は、図１２との対応部分に対応符号を付したものであり、基本構成は同様である。異なるのは、ファイアウォール１３０５の有するアドレスである。

【０２３５】本実施形態におけるファイアウォール１３０５が、外部ネットワークに接続しているネットワーク・インターフェースのアドレスは一つ、すなわち、アドレスＦｅである。一方、ファイアウォール１３０５が、内部ネットワークに接続しているネットワーク・インターフェースのアドレスは、複数のアドレスＦｉ１～Ｆｉｍ（ｍ＞１）である。

【０２３６】セッション管理部１３１０とセッション管理部１３１２は、互いに通信し、端末１３０７の認証と鍵交換をする。

【０２３７】セッション管理部１３１２は、セッション管理部１３１０へ、端末１３０７が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であること、サブネット管理サーバ１３０３のアドレスがＳであることを通知する。

【０２３８】セッション管理部１３１０は、Ｆｉ１～Ｆｉｍのうち、その時点で使用していないアドレスＦｉｊを求める。セッション管理部１３１０は、セッション管理部１３０８へ、端末１３０７が外部ネットワークへ移動したこと、移動前アドレスがＩ２であること、内部ホスト１３０１と端末１３０７の通信で使用するファイアウォール１３０５の内部アドレスがＦｉｊであること、鍵を通知する。

【０２３９】（Ｊ－２）第９の実施形態の動作

次に、第９の実施形態の動作を説明する。

【０２４０】（Ｊ－２－１）通信開始前の動作

まず、内部ホスト１３０１と端末１３０７が通信を開始するまでの動作を説明する。

【０２４１】セッション管理部１３１０とセッション管理部１３１２は、互いに通信し、端末１３０７の認証と鍵交換をする。

【０２４２】端末１３０７のセッション管理部１３１２は、セッション管理部１３１０へ、端末１３０７が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であること、サブネット管理サーバ１３０３のアドレスがＳであることを通知する。

【０２４３】ファイアウォール１３０５のセッション管理部１３１０は、Ｆｉ１～Ｆｉｍのうち、その時点で使用していないアドレスＦｉｊを求める。セッション管理部１３１０は、セッション管理部１３０８へ、端末１３０７が外部ネットワークへ移動したこと、移動前アドレスがＩ２であること、内部ホスト１３０１と端末１３０７の通信で使用するファイアウォール１３０５の内部アドレスがＦｉｊであること、鍵を通知する。

【０２４４】（Ｊ－２－２）通信開始後の動作

内部ホスト１３０１と端末１３０７が通信する場合の動作を説明する。第９の実施形態の動作のうち、第８の実施形態の動作とは異なる動作を説明する。

【０２４５】パケット１３１８は、内部ホスト１３０１から端末１３０７へ伝送されるパケット１３１７をカプセル化したパケットであり、その受信先アドレスはＦｉｊ、送信元アドレスはＳとなる。パケット１３１９は、このパケット１３１８のヘッダアドレスを書き換えたパケットであり、その受信先アドレスはＥ、送信元アドレスはＦｅとなる。

【０２４６】パケット１３２２は、端末１３０７から内部ホスト１３０１へ伝送されるパケット１３２１をカプセル化したパケットであり、その受信先アドレスはＦｅ、送信元アドレスはＥとなる。パケット１３２３は、このパケット１３２２のヘッダアドレスを書き換えたパケットであり、その受信先アドレスはＳ、送信元アドレスはＦｉｊとなる。

【０２４７】（Ｊ－２－２－１）内部ホストから端末への送信

まず、内部ホスト１３０１から端末１３０７にパケットを送信する場合の動作を説明する。

【０２４８】トンネリング処理部１３０９は、パケット１３１７を暗号処理しカプセル化しパケット１３１８を得る。この時、パケット１３１７の受信先アドレスがＩ２であるので、パケット１３１８の受信先アドレスをＦｉｊにする。

【０２４９】アドレス変換部１３２５は、パケット１３１８のヘッダのアドレスを書き換えパケット１３１９を得る。この時、パケット１３１８の受信先アドレスがＦｉｊであるので、パケット１３１９の受信先アドレスを

Ｅにする。

【０２５０】（Ｊ－２－２－２）端末から内部ホストへの送信

逆に、端末１３０７から内部ホスト１３０１にパケットを送信する場合の動作を説明する。

【０２５１】アドレス変換部１３２５は、パケット１３２２のヘッダのアドレスを書き換え、パケット１３２３を得る。この時、パケット１３２２の送信元アドレスがＥであるので、パケット１３２３の受信先アドレスをＳにする。

【０２５２】（Ｊ－３）第９の実施形態の効果

以上のように、第９の実施形態によれば、ファイアウォール１３０５に、複数の内部アドレスを割り当てるようにしたので、あるサブネット管理サーバ１３０３と同時に複数の端末１３０７が通信できるという効果が得られる。

【０２５３】（Ｋ）第１０の実施形態

続いて、第１０の実施形態を説明する。ところで、第９の実施形態では、ファイアウォールに、複数の内部アドレスを割り当てる必要がある。そこで、第１０の実施形態においては、パケットがサブネット管理サーバとどの端末の間の通信のパケットであるかをＳＰＩにより表すことにする。

【０２５４】（Ｋ－１）第１０の実施形態の構成

図１４は、第１０の実施形態の構成図である。図１４は、第８の実施形態の説明に用いた図１２との対応部分に対応符号を付して示したものであり、基本的な構成は同じである。

【０２５５】セッション管理部１４１０とセッション管理部１４１２は、互いに通信し、端末１４０７の認証と鍵交換をする。

【０２５６】端末１４０７のセッション管理部１４１２は、サブネット管理サーバ１４０３が端末１４０７へ送信するパケットのＳＰＩ（ここではＢとする。）を求める。セッション管理部１４１２は、セッション管理部１４１０へ、端末１４０７が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であること、サブネット管理サーバ１４０３のアドレスがＳであること、サブネット管理サーバ１４０３が端末１４０７へ送信するパケットのＳＰＩがＢであることを、通知する。

【０２５７】ファイアウォール１４０５のセッション管理部１４１０は、セッション管理部１４０８へ、端末１４０７が外部ネットワークへ移動したこと、移動前アドレスがＩ２であること、サブネット管理サーバ１４０３が端末１４０７へ送信するパケットのＳＰＩがＢであること、鍵を通知する。

【０２５８】セッション管理部１４０８は、端末１４０７が内部ホスト１４０１へ送信するパケットＳＰＩ（ここでは、Ａとする。）を求める。セッション管理部１４０８は、セッション管理部１４１０へ、端末１４０７が内部ホスト１４０１へ送信するパケットのＳＰＩがＡであることを通知する。セッション管理部１４１０はセッション管理部１４１２へ、端末１４０７が内部ホスト１４０１へ送信するパケットのＳＰＩがＡであることを通知する。

【０２５９】サブネット管理サーバ１４０３のトンネリング処理部１４０９は、パケット１４１７をカプセル化する時に、ＳＰＩをＢにする。

【０２６０】端末１４０７のトンネリング処理部１４１４は、パケット１４２１をカプセル化するときに、ＳＰＩをＡにする。

【０２６１】ファイアウォール１４０５のアドレス変換部１４２５は、ＳＰＩにより、パケットのヘッダのアドレスを書き換える。

【０２６２】（Ｋ－２）第１０の実施形態の動作

次に、第１０の実施形態の動作を説明する。なお、第１０の実施形態の動作のうち、第８の実施形態の動作とは異なる動作のみを説明する。

【０２６３】（Ｋ－２－１）通信開始後の動作

内部ホスト１４０１と端末１４０７が通信する場合の動作を説明する。

【０２６４】パケット１４１８は、内部ホスト１４０１から端末１４０７へ伝送されるパケット１４１７をカプセル化したパケットであり、その受信先アドレスはＦｉ、送信元アドレスはＳ、ＳＰＩはＢとなる。パケット１４１９は、このパケット１４１８のヘッダアドレスを書き換えたパケットであり、その受信先アドレスはＥ、送信元アドレスはＦｅ、ＳＰＩはＢとなる。

【０２６５】パケット１４２２は、端末１４０７から内部ホスト１４０１へ伝送されるパケット１４２１をカプセル化したパケットであり、その受信先アドレスはＦｅ、送信元アドレスはＥ、ＳＰＩはＡとなる。パケット１４２３は、パケット１４２２のヘッダのアドレスを書き換えたパケットであり、受信先アドレスはＳ、送信元アドレスはＦｉ、ＳＰＩはＡとなる。

【０２６６】（Ｋ－２－１－１）内部ホストから端末への送信

まず、内部ホスト１４０１から端末１４０７にパケットを送信する場合の動作を説明する。

【０２６７】トンネリング処理部１４０９は、パケット１４１７を暗号処理しカプセル化しパケット１４１８を得る。この時、パケット１４１７の受信先アドレスがＩ２であるので、ＳＰＩをＢにする。アドレス変換部１４２５は、パケット１４１８のヘッダのアドレスを書き換え、パケット１４１９を得る。この時、パケット１４１８のＳＰＩがＢであるので、パケット１４１９の受信先アドレスをＥとする。

【０２６８】（Ｋ－２－１－２）端末から内部ホストへの送信

逆に、端末１４０７から内部ホスト１４０１にパケットを送信する場合の動作を説明する。

【０２６９】アドレス変換部１４２５は、パケット１４２２のヘッダのアドレスを書き換え、パケット１４２３を得る。この時、パケット１４２２の送信元アドレスがＥであるので、パケット１４２３の受信先アドレスをＳとする。

【０２７０】（Ｋ－３）第１０の実施形態の効果

以上のように、第１０の実施形態によれば、パケットのヘッダに書き込まれているＳＰＩにより、パケットがどのサブネット管理サーバとどの端末の間の通信のパケットであるかを表すようにしたので、ファイアウォールに複数の内部アドレスを割り当てなくても、あるサブネット管理サーバと複数の端末が同時に通信できるようになるという効果が得られる。

【０２７１】（Ｌ）第１１の実施形態

続いて、第１１の実施形態を説明する。ところで、第７、第８、第９、第１０の実施形態では、内部ネットワークのあるサブネットに位置する端末を、内部ネットワークの他のサブネットへ移動すると、端末のアドレスが変化するので、端末は移動前のサービス利用権限で内部ホストが提供するサービスを利用できなくなる。そこで、次の構成を考える。なお、第１１の実施形態では、端末が外部ネットワークに移動する場合に係る構成及び動作は、第７の実施形態の場合と同様である。

【０２７２】（Ｌ－１）第１１の実施形態の構成

図１５は、第１１の実施形態の構成図である。図１５には、内部ネットワークのあるサブネットに位置する端末を、内部ネットワークの他のサブネットへ移動する場合に係る構成要素を示している。また、図１５には、端末を外部ネットワークへ移動する場合に係る構成要素の一部を示す。従って、図１５に示されている、内部ホスト１５０１、「通信路Ａ」１５０２、サブネット管理サーバ１５０３、「通信路Ｄ」１５０４、端末１５０５の他に、不図示のファイアウォールがある。

【０２７３】本実施形態に係るサブネット管理サーバ１５０３は、外部セッション管理部１５０６、内部セッション管理部１５０７、トンネリング処理部１５０８を構成要素としてもつ。

【０２７４】本実施形態に係る端末１５０５は、内部セッション管理部１５０９、外部セッション管理部１５１０、移動前情報記憶部１５１１、トンネリング処理部１５１２を構成要素としてもつ。

【０２７５】サブネット管理サーバ１５０３は、サブネットＡに位置する。

【０２７６】端末１５０５は、内部ネットワークでの移動前にサブネットＡに位置し、内部ネットワークでの移動後にサブネットＢに位置する。

【０２７７】「通信路Ａ」１５０２は、内部ホスト１５０１とサブネット管理サーバ１５０３の間の通信路である。すなわち、「通信路Ａ」１５０２は、内部ネットワークの通信路である。「通信路Ｄ」１５０４は、サブネット管理サーバ１５０３と端末１５０５の間の通信路である。すなわち、「通信路Ｄ」１５０４は、内部ネットワークの通信路である。

【０２７８】サブネット管理サーバ１５０３と端末１５０５の間にはトンネル１５１３を設ける。

【０２７９】内部セッション管理部１５０７と内部セッション管理部１５０９は、互いに通信し、端末１５０５の認証と鍵交換をする。

【０２８０】内部セッション管理部１５０９は、内部セッション管理部１５０７へ、端末１５０５が内部ネットワークの他のサブネットに移動したこと、移動後のアドレスがＩ２'であること、移動前アドレスがＩ２であることを通知する。

【０２８１】トンネリング処理部１５０８は、内部セッション管理部１５０７が交換した鍵を使用して、端末１５０５宛てのパケットを暗号処理してカプセル化する。

【０２８２】また、トンネリング処理部１５０８は、外部セッション管理部１５０６が交換した鍵を使用して、外部ネットワークに移動した端末宛てのパケットを暗号処理してカプセル化する。トンネリング処理部１５０８は、内部ホスト１５０１宛てのパケットを脱カプセル化し復号処理する。

【０２８３】トンネリング処理部１５１２は、内部セッション管理部１５０９が交換した鍵を使用して、内部ホスト１５０１宛てのパケットを暗号処理しカプセル化する。また、トンネリング処理部１５１２は、外部セッション管理部１５１０が交換した鍵を使用して、内部ホスト１５０１宛てのパケットを暗号処理しカプセル化する。トンネリング処理部１５１２は、端末１５０５宛てのパケットを脱カプセル化し復号処理する。

【０２８４】移動前情報記憶部１５１１は、端末１５０５の移動前アドレスＩ２とサブネット管理サーバ１５０３のアドレスＳを記憶する。

【０２８５】第７の実施形態と同様に、ファイアウォールの構成要素は、セッション管理部とアクセス制御部である。サブネット管理サーバ１５０３とファイアウォールの間には、「通信路Ｂ」とトンネルがある。ファイアウォールと外部ネットワークに移動した端末の間には、「通信路Ｃ」とトンネルがある。

【０２８６】外部セッション管理部１５１０とファイアウォールのセッション管理部は、互いに通信し、外部ネットワークに移動した端末の認証と鍵交換をする。外部セッション管理部１５１０は、ファイアウォールのセッション管理部へ、端末が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であることを、サブネット管理サーバ１５０３のアドレスがＳであることを通知する。

【０２８７】ファイアウォールのセッション管理部は、

外部セッション管理部１５０６へ、端末が外部ネットワークへ移動したこと、移動後のアドレスがＥであること、移動前アドレスがＩ２であること、鍵を通知する。

【０２８８】（Ｌ－２）第１１の実施形態の動作

次に、第１１の実施形態の動作を説明する。なお、第１１の実施形態の動作のうち、第７の実施形態の動作とは異なる動作のみを説明する。

【０２８９】（Ｌ－２－１）通信開始前の動作

内部ホスト１５０１と端末１５０５の通信の開始における動作を説明する。

【０２９０】内部セッション管理部１５０７と内部セッション管理部１５０９は、互いに通信し、端末１５０５の認証と鍵交換をする。

【０２９１】端末１５０５の内部セッション管理部１５０９は、セッション管理部１５０７へ、端末１５０５が内部ネットワークの他のサブネットに移動したこと、移動後のアドレスがＩ２’であること、移動前アドレスがＩ２であることを通知する。

【０２９２】（Ｌ－２－２）通信開始後の動作

次に、内部ホスト１５０１と端末１５０５が通信をする時の動作を説明する。

【０２９３】内部ホスト１５０１から端末１５０５へ伝送されるパケット１５１４の受信先アドレスはＩ２、送信元アドレスはＩ１となる。このパケット１５１４をカプセル化したパケット１５１５の受信先アドレスはＩ２’、送信元アドレスはＳとなる。パケット１５１６は、パケット１５１４と同一である。

【０２９４】端末１５０５から内部ホスト１５０１へ伝送されるパケット１５１７の受信先アドレスはＩ１、送信元アドレスはＩ２となる。このパケット１５１７をカプセル化したパケット１５１８の受信先アドレスはＳ、送信元アドレスはＩ２’となる。パケット１５１９は、パケット１５１７と同一である。

【０２９５】（Ｌ－２－２－１）内部ホストから端末への送信

まず、内部ホスト１５０１から端末１５０５へパケットを送信する場合の動作を説明する。

【０２９６】サブネット管理サーバ１５０３のトンネリング処理部１５０８は、パケット１５１４を暗号処理しカプセル化しパケット１５１５を得る。この時、パケット１５１４の受信先アドレスがＩ２であるので、パケット１５１５の受信先アドレスをＩ２’にする。

【０２９７】（Ｌ－２－２－２）端末から内部ホストへの送信

逆に、端末１５０５から内部ホスト１５０１へパケットを送信する場合の動作を説明する。

【０２９８】端末１５０５のトンネリング処理部１５１２は、パケット１５１７を暗号処理しカプセル化しパケット１５１８を得る。この時、サブネット管理サーバ１５０３のアドレスがＳであるので、パケット１５１８の受信先アドレスをＳにする。

【０２９９】外部ネットワークに移動した端末と内部ホストの通信に関しては、第７の実施形態の動作と同様である。

【０３００】（Ｌ－３）第１１の実施形態の効果

以上のように、第１１の実施形態によれば、サブネット管理サーバと、内部ネットワークの他のサブネットへ移動した端末の間にトンネルを設けるので、端末が内部ネットワークの他のサブネットに移動しても、内部ホストが提供するサービスを移動前のサービス利用権限で利用できるという効果が得られる。

【０３０１】また、第１１の実施形態では、あるサブネット管理サーバ１５０３と複数の端末１５０５が同時に通信可能である。

【０３０２】（Ｍ）第１２の実施形態

続いて、第１２の実施形態を説明する。ところで、第１１の実施形態では、端末１５０５がトンネリングの処理をする必要がある。そこで、次の構成を考える。なお、第１２の実施形態では、端末が外部ネットワークに移動する場合に係る構成、動作は、第７の実施形態と同じである。

【０３０３】（Ｍ－１）第１２の実施形態の構成

図１６は、第１２の実施形態の構成図である。図１６には、内部ネットワークのあるサブネットに位置する端末を、内部ネットワークの他のサブネットへ移動する場合に係る構成要素を示す。また、図１６には、端末を外部ネットワークへ移動する場合に係る構成要素の一部を示す。従って、図１６に示されている、内部ホスト１６０１、「通信路Ａ」１６０２、「サブネット管理サーバＡ」１６０３、「通信路Ｅ」１６０４、「サブネット管理サーバＢ」１６０５、「通信路Ｆ」１６０６、端末１６０７、他に、不図示のファイアウォールがある。

【０３０４】ここで、「サブネット管理サーバＡ」１６０３は、サブネットＡに位置する。「サブネット管理サーバＢ」１６０５は、サブネットＢに位置する。端末１６０７が移動前に位置するサブネットは、サブネットＡである。端末１６０７が移動後に位置するサブネットは、サブネットＢである。

【０３０５】「サブネット管理サーバＡ」１６０３は、外部セッション管理部１６０８、内部セッション管理部１６０９、トンネリング処理部１６１０を構成要素とする。一方、「サブネット管理サーバＢ」１６０５は、内部セッション管理部１６１１、外部セッション管理部１６１２、トンネリング処理部１６１３を構成要素とする。

【０３０６】端末１６０７は、内部セッション管理部１６１４、外部セッション管理部１６１５、移動前情報記憶部１６１６、トンネリング処理部１６１７を構成要素とする。

【０３０７】内部ホスト１６０１と「サブネット管理サ

ーバＡ」１６０３の間には「通信路Ａ」１６０２を設ける。この「通信路Ａ」１６０２は、内部ネットワークの通信路である。「サブネット管理サーバＡ」１６０３と「サブネット管理サーバＢ」１６０５の間には「通信路Ｅ」１６０４を設ける。この「通信路Ｅ」１６０４は、内部ネットワークの通信路である。「サブネット管理サーバＢ」１６０５と端末１６０７の間には「通信路Ｆ」１６０６を設ける。この「通信路Ｆ」１６０６は、内部ネットワークの通信路である。

【０３０８】「サブネット管理サーバＡ」１６０３と「サブネット管理サーバＢ」１６０５の間にはトンネル１６１８を設ける。

【０３０９】内部セッション管理部１６０９と内部セッション管理部１６１４は、互いに通信し、端末１６０７の認証と鍵交換をする。

【０３１０】内部セッション管理部１６１４は、内部セッション管理部１６０９へ、端末１６０７が内部ネットワークの他のサブネットに移動したこと、移動後のアドレスがＩ２’であること、移動前アドレスがＩ２であることを通知する。

【０３１１】内部セッション管理部１６０９は、端末１６０７の移動後のアドレスＩ２’から、「サブネット管理サーバＢ」のアドレスＳ２を求める。内部セッション管理部１６０９は、内部セッション管理部１６１１へ、端末１６０７がサブネットＢへ移動したこと、端末１６０７の移動前アドレスがＩ２であること、「サブネット管理サーバＡ」のアドレスがＳ１であること、鍵を通知する。

【０３１２】トンネリング処理部１６１０は、内部セッション管理部１６０９が交換した鍵を使用して、端末１６０７宛てのパケットを暗号処理してカプセル化する。

【０３１３】また、トンネリング処理部１６１０は、ファイアウォールのセッション管理部が外部セッション管理部１６０８に通知した鍵を使用して、外部ネットワークへ移動した端末宛てのパケットを暗号処理してカプセル化する。トンネリング処理部１６１０は、内部ホスト１６０１宛てのパケットを脱カプセル化し復号処理する。

【０３１４】トンネリング処理部１６１３は、内部セッション管理部１６０９が内部セッション管理部１６１１に通知した鍵を使用して、内部ホスト１６０１宛てのパケットを暗号処理しカプセル化する。また、トンネリング処理部１６１３は、ファイアウォールのセッション管理部が外部セッション管理部１６１２に通知した鍵を使用して、外部ネットワークへ移動した端末宛てのパケットを暗号処理しカプセル化する。トンネリング処理部１６１３は、端末１６０７宛てのパケットを脱カプセル化し復号処理する。

【０３１５】トンネリング処理部１６１７は、外部セッション管理部１６１５が交換した鍵を使用して、内部ホスト１６０１宛てのパケットを暗号処理しカプセル化する。また、トンネリング処理部１６１７は、外部ネットワークに移動した端末宛てのパケットを脱カプセル化し復号処理する。

【０３１６】移動前情報記憶部１６１６は、端末１６０７の移動前アドレスＩ２と「サブネット管理サーバＡ」１６０３のアドレスＳ１を記憶する。

【０３１７】第７の実施形態と同様に、ファイアウォールの構成要素は、セッション管理部とアクセス制御部である。「サブネット管理サーバＡ」１６０３とファイアウォールの間には、「通信路Ｂ」とトンネルがある。「サブネット管理サーバＢ」１６０５とファイアウォールの間には別の通信路と別のトンネルがある。ファイアウォールと外部ネットワークに移動した端末の間には、「通信路Ｃ」とトンネルがある。

【０３１８】（Ｍ－２）第１２の実施形態の動作

次に、第１２の実施形態の動作を説明する。なお、第１２の実施形態の動作のうち、第７の実施形態の動作とは異なる動作のみを説明する。

【０３１９】（Ｍ－２－１）通信開始前の動作

まず、内部ホスト１６０１と端末１６０７の通信の開始における動作を説明する。

【０３２０】「サブネット管理サーバＡ」１６０３の内部セッション管理部１６０９と端末１６０７の内部セッション管理部１６１４は、互いに通信し、端末１６０７の認証と鍵交換をする。

【０３２１】端末１６０７の内部セッション管理部１６１４は、内部セッション管理部１６０９へ、端末１６０７が内部ネットワークの他のサブネットに移動したこと、移動後のアドレスがＩ２’であること、移動前アドレスがＩ２であることを通知する。

【０３２２】「サブネット管理サーバＡ」１６０３の内部セッション管理部１６０９は、端末１６０７の移動後のアドレスＩ２’から、「サブネット管理サーバＢ」のアドレスＳ２を求める。内部セッション管理部１６０９は、内部セッション管理部１６１１へ、端末１６０７がサブネットＢへ移動したこと、端末１６０７の移動前アドレスがＩ２であること、サブネット管理サーバＡ１６０３のアドレスがＳ１であること、鍵を通知する。ここで、内部セッション管理部１６０９と内部セッション管理部１６１４が通信する時に使用する通信路は、「通信路Ｅ」１６０４と「通信路Ｆ」１６０６であっても、図１６に示さない別の通信路であってもよい。

【０３２３】（Ｍ－２－２）通信開始後の動作

次に、内部ホスト１６０１と端末１６０７が通信をする時の動作を説明する。

【０３２４】内部ホスト１６０１から端末１６０７へ伝送されるパケット１６１９の受信先アドレスはＩ２、送信元アドレスはＩ１となる。このパケット１６１９をカプセル化したパケット１６２０の受信先アドレスはＳ

２、送信元アドレスはＳ１となる。パケット１６２１は、パケット１６１９と同一である。

【０３２５】端末１６０７から内部ホスト１６０１へ伝送されるパケット１６２２の受信先アドレスはＩ１、送信元アドレスはＩ２となる。このパケット１６２２をカプセル化したパケット１６２３の受信先アドレスはＳ１、送信元アドレスはＳ２となる。パケット１６２４は、パケット１６２２と同一である。

【０３２６】（Ｍ－２－２－１）内部ホストから端末への送信

まず、内部ホスト１６０１から端末１６０７へパケットを送信する場合の動作を説明する。トンネリング処理部１６１０は、パケット１６１９を暗号処理しカプセル化し、パケット１６２０を得る。この時、パケット１６１９の受信先アドレスがＩ２であるので、パケット１６２０の受信先アドレスをＳ２にする。

【０３２７】（Ｍ－２－２－２）端末から内部ホストへの送信

逆に、端末１６０７から内部ホスト１６０１へパケットを送信する場合の動作を説明する。

【０３２８】トンネリング処理部１６１３は、パケット１６２２を暗号処理しカプセル化しパケット１６２３を得る。この時、トンネリング処理部１６１３は、パケット１６２２の送信元アドレスがＩ２であるので、パケット１６２３の受信先アドレスをＳ１にする。

【０３２９】（Ｍ－３）第１２の実施形態の効果

以上のように、第１２の実施形態によれば、サブネット管理サーバの間にトンネルを設けるので、端末がトンネリングの処理をしないので、端末の負荷を軽減できるという効果が得られる。

【０３３０】また、第１２の実施形態では、複数のサブネット管理サーバどうしが同時に通信可能であり、また、複数の内部ホスト１６０１と複数の端末１６０７とも同時に通信可能である。

【０３３１】（Ｎ）他の実施形態

(N-1) なお、上述の各実施形態においては、内部ネットワークに位置する端末を外部ネットワークに移動した場合におけるサービスの利用権限について説明したが、内部ネットワークに一度も位置しないが、内部ネットワーク上のアドレスが割り当てられており、かつ、そのアドレスを記憶している端末についても本システムを適用することができる。すなわち、かかる端末についても、内部ホストのサービスを内部ネットワークでのアドレスに基づくサービス利用権限で利用することができる。

【０３３２】(N-2) また、上述の各実施形態においては、端末が内部ホストのサービスを利用することを前提として説明したが、内部ネットワークのいずれかのコンピュータが、端末の外部ネットワークでのアドレスを記憶するならば、内部ホストが端末のサービスを利用することもできる。

【０３３３】(N-3) また、上述の各実施形態においては、パケットを暗号処理する場合についてのみ述べたが、パケットの暗号処理とパケットの認証処理をすることもできる。また、パケットを暗号処理せず、パケットの認証処理だけをすることもできる。パケットを認証する方式には、従来技術の上記文献に示されるＡＨ（Authentication Header）がある。

【０３３４】(N-4) また、上述の各実施形態においては、パケットを暗号処理する場合について述べたが、トンネリング処理部で複数の暗号処理のアルゴリズムを使えるようにすると、パケットのヘッダのアドレスにより、暗号処理のアルゴリズムを変える通信方式、パケットのヘッダのＳＰＩにより、暗号処理のアルゴリズムを変える通信方式も実施可能である。ここで、暗号処理のアルゴリズムには、恒等写像を含むものとする。通信路がセキュリティの面で安全であるとみなせる場合には、暗号処理のアルゴリズムは恒等写像でよい。また、通信する情報が既に暗号化されている場合も、暗号処理のアルゴリズムは恒等写像でよい。

【０３３５】(N-5) また、第５、第１０の実施形態においては、パケットのヘッダのＳＰＩ（使用する暗号アルゴリズムや鍵などのセキュリティに関係するパラメータを表す）を利用して、パケットのヘッダのアドレスを書き換える場合について述べたが、パケットのヘッダに、パケットが通過するトンネルの両端のアドレスを表すフィールドを設け、そのフィールドの値を利用するようにしても、パケットのヘッダのアドレスを書き換えることができる。

【０３３６】(N-6) また、第２～第１２の実施形態においては、トンネルの端に位置する内部ホスト又はサブネット管理サーバで暗号処理と復号処理とを行っているが、暗号処理と復号処理を、トンネル内部の端以外の位置のコンピュータで行うこともできる。暗号処理と復号処理を、トンネル内部の端以外の位置のコンピュータで行うと、内部ホスト、サブネット管理サーバの負荷を下げることができる。なお、第２～第１２の実施形態においては、トンネル内部の端以外の位置のコンピュータは、ファイアウォールである。

【０３３７】(N-7) また、第２～第１２の実施形態においては、外部ネットワークに移動した端末の認証と鍵交換を、ファイアウォールのセッション管理部が行っているが、外部ネットワークに移動した端末の認証と鍵交換を、内部ホスト又はサブネット管理サーバのセッション管理部が行うこともできる。外部ネットワークに移動した端末の認証と鍵交換を、内部ホスト又はサブネット管理サーバのセッション管理部が行うと、ファイアウォールの負荷を下げることができる。

【０３３８】(N-8) また、上述の各実施形態においては、ファイアウォール、内部ホスト、サブネット管理サーバのいずれかと端末が鍵交換をする場合を例に説明し

たが、鍵交換をする代わりに、固定の鍵を使用することもできる。

【０３３９】

【発明の効果】以上のように、第１の発明によれば、外部ネットワークに位置する端末が、ファイアウォールを介して内部ネットワークの内部ホストと通信する形態の通信システムにおいて、端末に、移動前に又は予め内部ネットワークにおいて割り当てられた端末アドレスを記憶するアドレス記憶手段を備えるようにする。これにより、外部ネットワークに位置する端末であっても内部ネットワークで割り当てられた端末アドレスを記憶する端末については、内部ホスト側において、当該端末に提供し得るサービスの利用権限を判別することが可能となる。その結果、特定の端末については、外部ネットワークに位置する場合にも、内部ネットワークに位置する場合と同じ利用権限でのサービスを受けることができる通信システムを実現できる。

【０３４０】また、第２の発明によれば、内部ネットワーク内のあるサブネットに位置する端末が、当該ネットワーク内で内部ホストと通信する形態の通信システムにおいて、(1) 端末に、同じネットワーク内のあるサブネットから他のサブネットへ移動した後も、移動前に割り当てられた端末アドレスを記憶し続けるアドレス記憶手段を備えると共に、(2) 端末及び内部ホストに、当該移動があった場合に、アドレス記憶手段が記憶している移動前の端末アドレスと同一のアドレスを有するパケットを、カプセル化後、端末及び内部ホストの間に形成したトンネルを介して入出力するトンネリング処理手段を備えるようにする。これにより、端末が、内部ネットワーク内のあるサブネットから他のサブネットに端末が移動した場合にも、移動前のサブネットで許容されていたのと同じ利用権限でサービスを受けることができるようになる。

【０３４１】さらに、第３の発明によれば、内部ネットワーク内のあるサブネットに位置する端末が、当該ネットワーク内の内部ホストと通信する形態の通信システムにおいて、(1) 端末に、同一ネットワーク内のあるサブネットから他のサブネットへ移動した後も、移動前に割り当てられた端末アドレスを記憶し続けるアドレス記憶手段を備えると共に、(2) 端末及び当該端末が移動前に位置したサブネットのサブネット管理サーバは、当該移動があった場合に、アドレス記憶手段が記憶している移動前の端末アドレスと同一のアドレスを有するパケットを、カプセル化後、端末及びサブネット管理サーバ間に形成したトンネルを介して入出力するトンネリング処理手段を備えるようにする。これにより、端末が、内部ホストごとに各端末までのトンネルを設けなくて良くなる。

【０３４２】さらに、第４の発明によれば、内部ネットワーク内のあるサブネットに位置する端末が、当該ネットワーク内の内部ホストと通信する形態の通信システムにおいて、(1) 端末に、同一ネットワーク内のあるサブネットから他のサブネットへ移動した後も、移動前に割り当てられた端末アドレスを記憶し続けるアドレス記憶手段を備えると共に、(2) 端末の移動の前後に係る各サブネットのサブネット管理サーバは、当該移動があった場合に、アドレス記憶手段が記憶している移動前の端末アドレスと同一のアドレスを有するパケットを、カプセル化後、当該サブネット管理サーバ間に形成したトンネルを介して入出力するトンネリング処理手段を備えるようにする。これにより、端末がトンネリング処理をせずに済み、その分、端末の負荷を軽減することができる。

【図面の簡単な説明】

【図１】第１の実施形態に係る通信システムの構成例を示すブロック図である。

【図２】従来のパケット構成を示す説明図である。

【図３】従来の通信システムの構成を示すブロック図である。

【図４】各実施形態で使用するパケット構成を示す説明図である。

【図５】一部の実施形態で使用するパケット構成を示す説明図である。

【図６】第２の実施形態に係る通信システムの構成例を示すブロック図である。

【図７】第３の実施形態に係る通信システムの構成例を示すブロック図である。

【図８】第４の実施形態に係る通信システムの構成例を示すブロック図である。

【図９】第５の実施形態に係る通信システムの構成例を示すブロック図である。

【図１０】第６の実施形態に係る通信システムの構成例を示すブロック図である。

【図１１】第７の実施形態に係る通信システムの構成例を示すブロック図である。

【図１２】第８の実施形態に係る通信システムの構成例を示すブロック図である。

【図１３】第９の実施形態に係る通信システムの構成例を示すブロック図である。

【図１４】第１０の実施形態に係る通信システムの構成例を示すブロック図である。

【図１５】第１１の実施形態に係る通信システムの構成例を示すブロック図である。

【図１６】第１２の実施形態に係る通信システムの構成例を示すブロック図である。

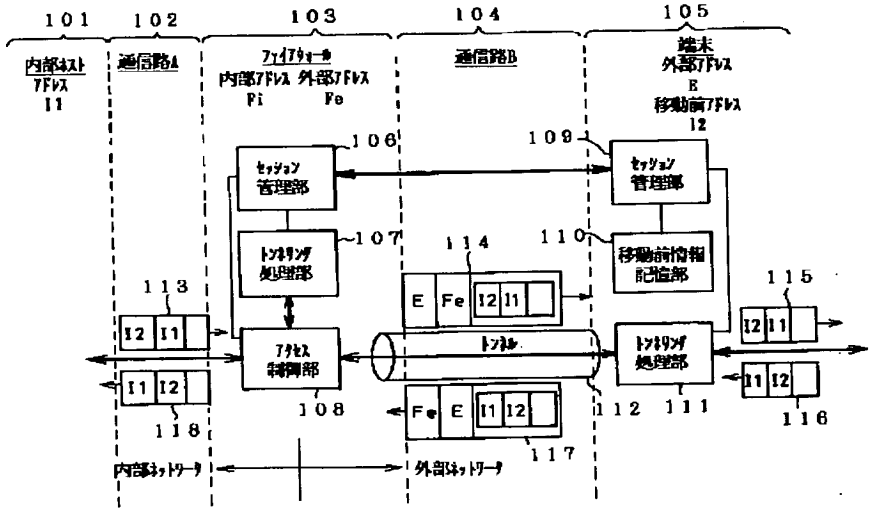
【符号の説明】

５０１、６０１…内部ホスト、５０３、６０３～９０３、１１０５、１２０５１３０５、１４０５…ファイアウォール、５０５、６０５～９０５、１００３、１１０７、１２０７～１４０７、１５０５、１６０７…端末、１１０３、１２０３～１６０３、１６０５…サブネット

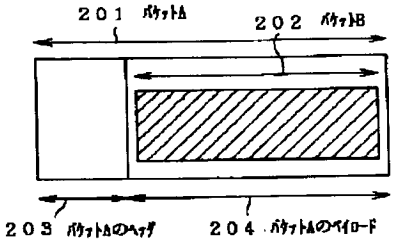
管理サーバ、５１０、６１１、７１１、８１１、９１１、１００９、１１１３、１２１３、１３１３、１４１３、１５１１、１６１６…移動前情報記憶部、１００５、１００７、１５０７、１５０９、１６０９、１６１

１、１６１４…内部セッション管理部、１００４、１００８、１５０６、１５１０、１６０８、１６１２、１６１５…外部セッション管理部。

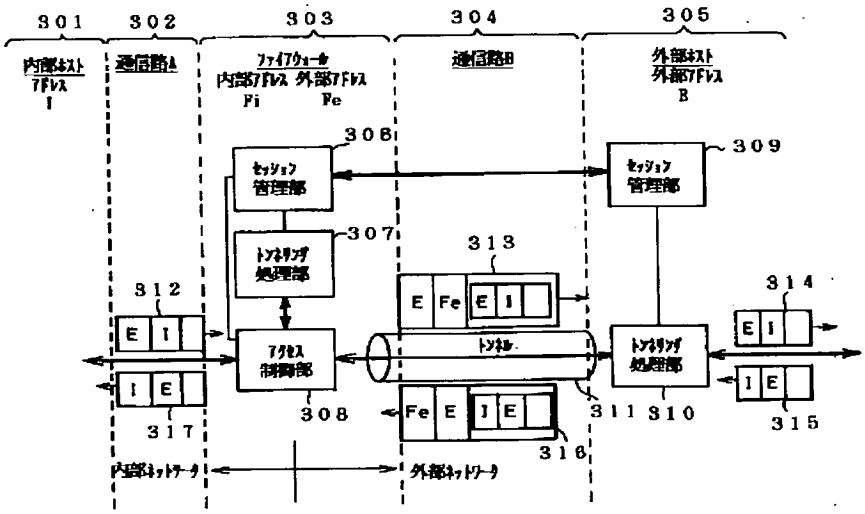
【図１】



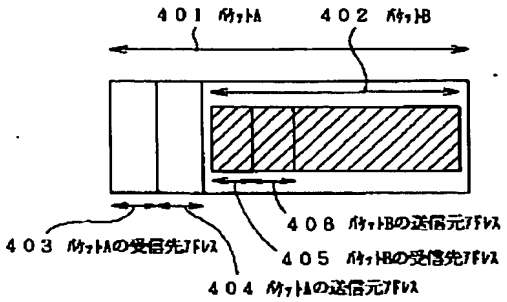
【図２】



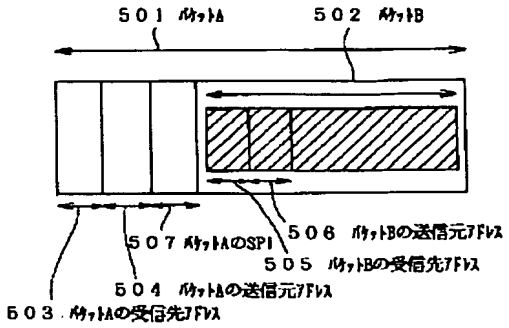
【図３】



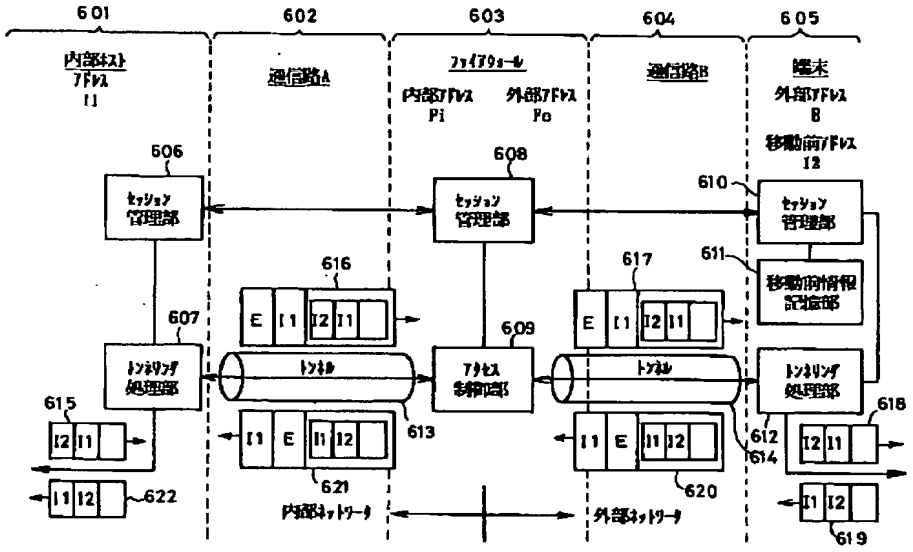
【図４】


４０１ パケットA
４０２ パケットB
４０３ パケットAの受信先アドレス
４０４ パケットAの送信元アドレス
４０５ パケットBの受信先アドレス
４０８ パケットBの送信元アドレス

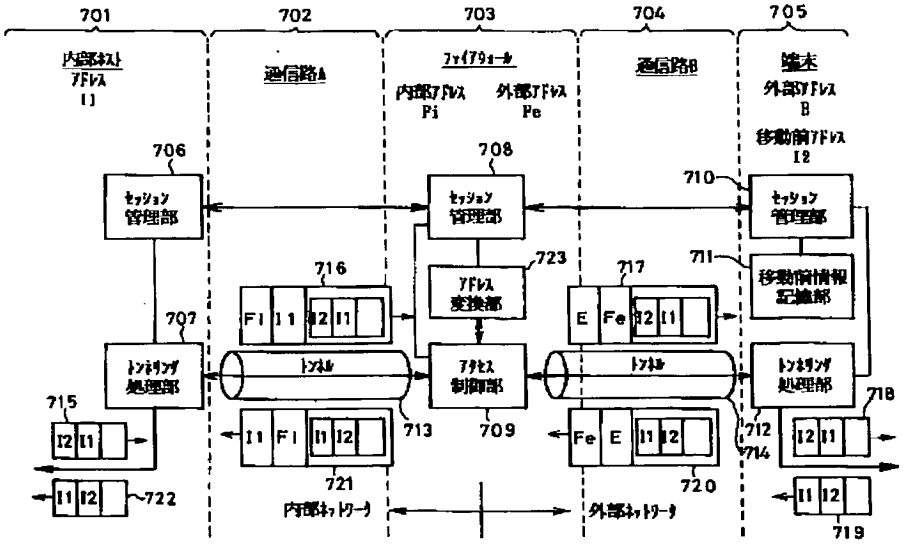
【図５】


５０１ パケットA
５０２ パケットB
５０３ パケットAの受信先アドレス
５０４ パケットAの送信元アドレス
５０５ パケットBの受信先アドレス
５０６ パケットBの送信元アドレス
５０７ パケットAのSPI

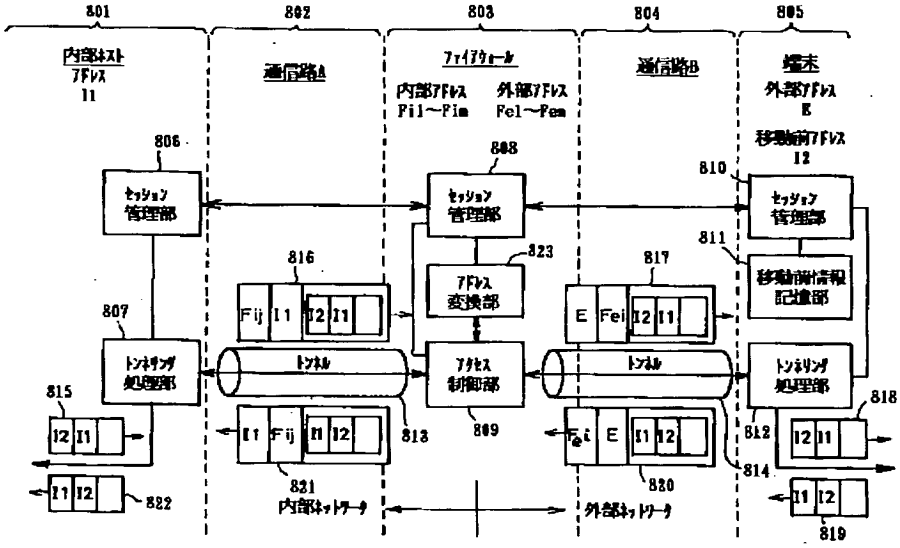
【図６】


601
602
603
604
605
内部ホストアドレス I1
通信路A
ファイアウォール
内部アドレス Pi
外部アドレス Po
通信路B
端末
外部アドレス B
移動前アドレス I2
606
608
610
611
616
617
607
609
615
613
612
614
618
621
620
622
619
内部ネットワーク
外部ネットワーク

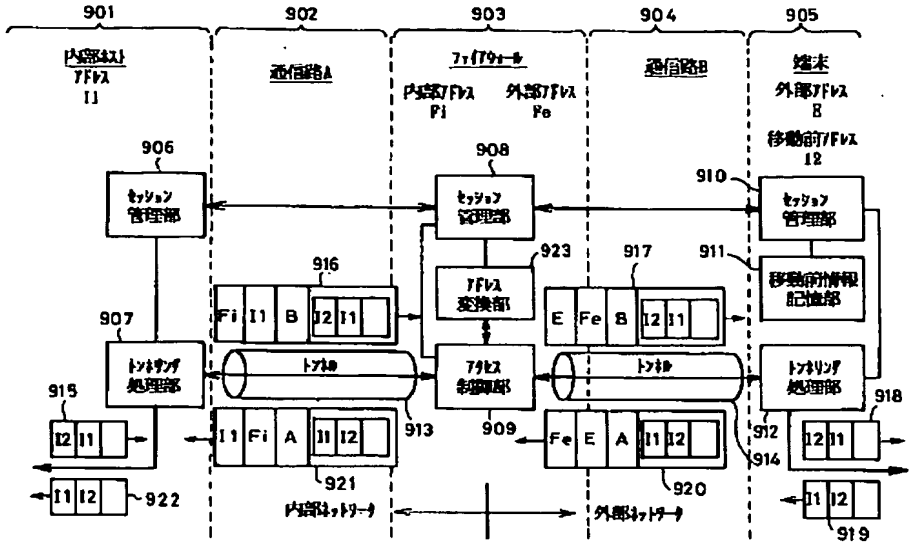
【図７】


701
702
703
704
705
内部ホスト アドレス I1
通信路A
ファイアウォール
内部アドレス Pi
外部アドレス Pe
通信路B
端末
外部アドレス E
移動前アドレス I2
706
708
710
セッション管理部
セッション管理部
セッション管理部
716
723
717
711
F I 1 1 I2 I1
アドレス変換部
E Fe I2 I1
移動前情報記憶部
707
トンネリング処理部
トンネル
アクセス制御部
トンネル
トンネリング処理部
715
718
I2 I1
I1 F I I1 I2
713
709
Fe E I1 I2
712
714
I2 I1
I1 I2
722
721
720
I1 I2
719
内部ネットワーク
外部ネットワーク

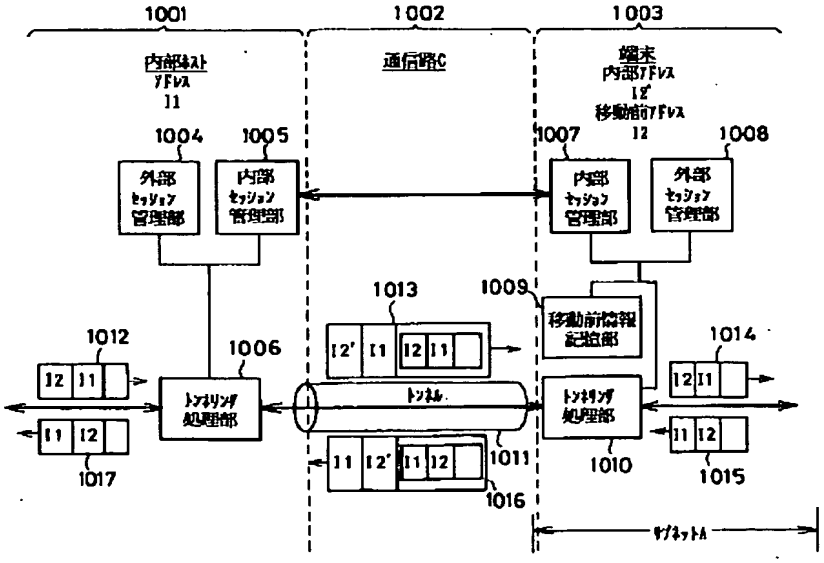
【図８】


801
802
803
804
805
内部ホスト アドレス I1
通信路A
ファイアウォール
内部アドレス Pi1～Pim
外部アドレス Fe1～Fem
通信路B
端末
外部アドレス E
移動前アドレス I2
806
808
810
セッション管理部
セッション管理部
セッション管理部
816
823
817
811
Fij I1 I2 I1
アドレス変換部
E Fei I2 I1
移動前情報記憶部
807
トンネリング処理部
トンネル
アクセス制御部
トンネル
トンネリング処理部
815
818
I2 I1
I1 Fij I1 I2
813
809
Fei E I1 I2
812
814
I2 I1
I1 I2
822
821
820
I1 I2
819
内部ネットワーク
外部ネットワーク

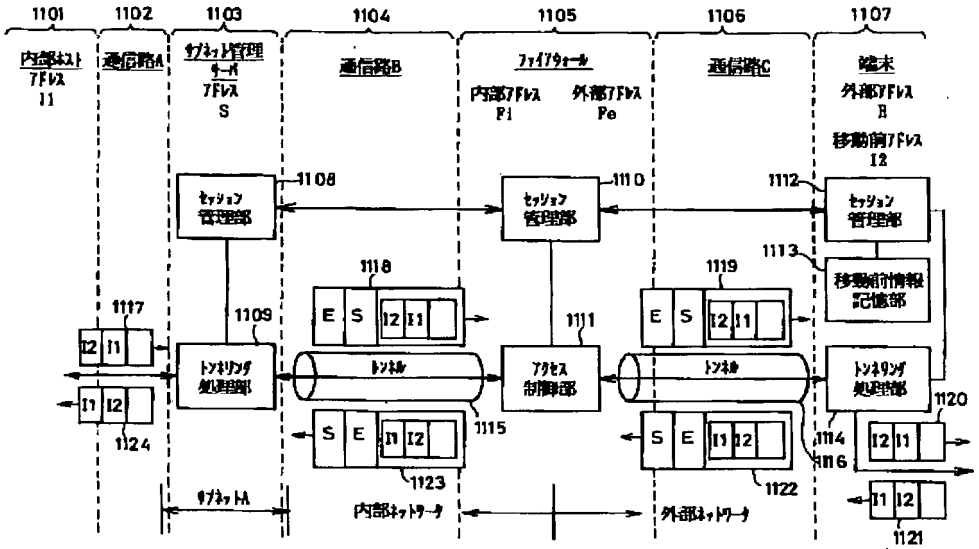
【図９】


901
902
903
904
905
通信路A
通信路B
906
908
910
907
916
923
917
911
915
913
909
912
914
918
921
920
922
919

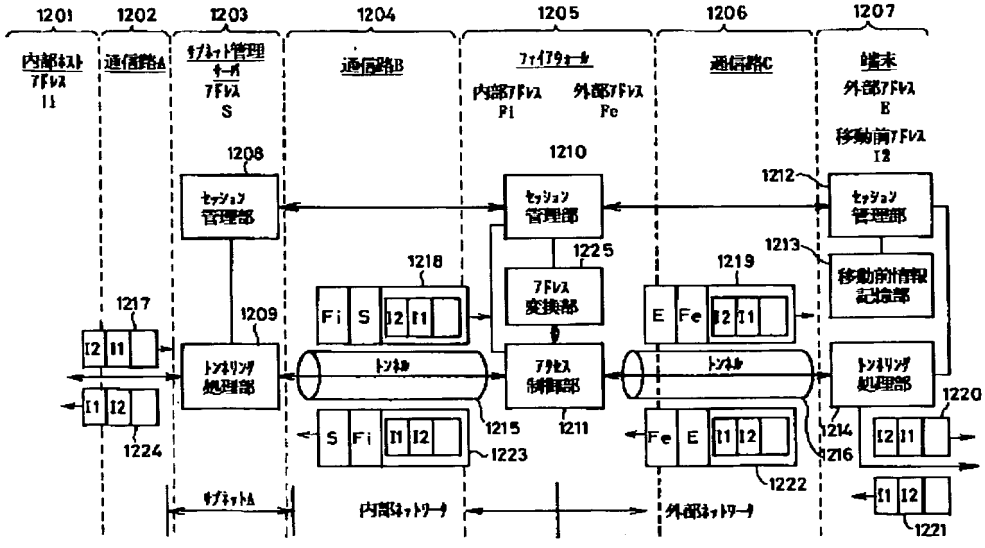
【図１０】


1001
1002
1003
通信路C
1004
1005
1007
1008
1013
1009
1012
1006
1014
1011
1010
1015
1017
1016

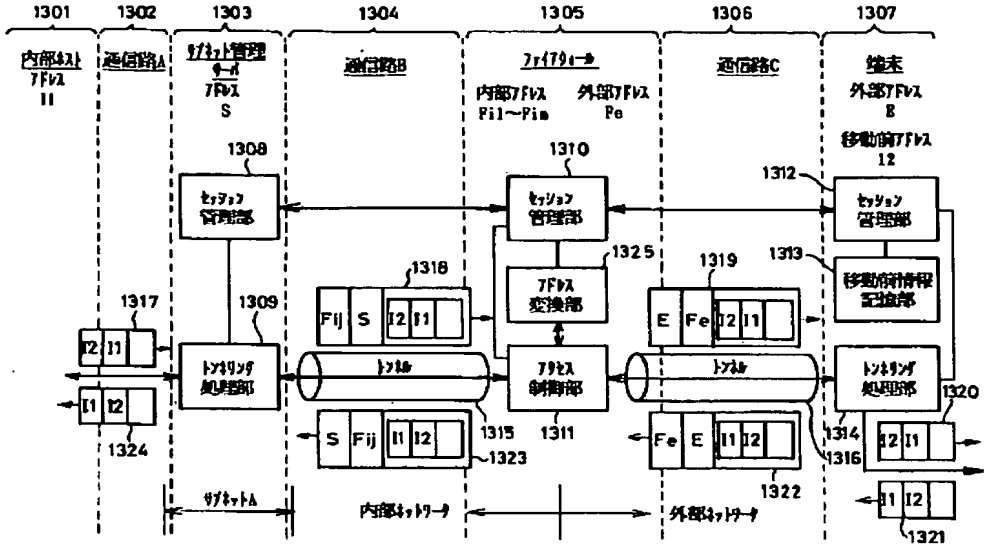
【図１１】


1101
1102
1103
1104
1105
1106
1107
内部ホスト
アドレス
I1
通信路A
サブネット管理
サーバ
アドレス
S
通信路B
ファイアウォール
内部アドレス
Pi
外部アドレス
Pe
通信路C
端末
外部アドレス
E
移動前アドレス
I2
セッション
管理部
1108
1110
1112
1113
移動前情報
記憶部
1118
1119
1117
1109
1111
E
S
I2
I1
トンネリング
処理部
トンネル
アクセス
制御部
1115
1120
1114
1116
1124
1123
1122
1121
サブネットA
内部ネットワーク
外部ネットワーク

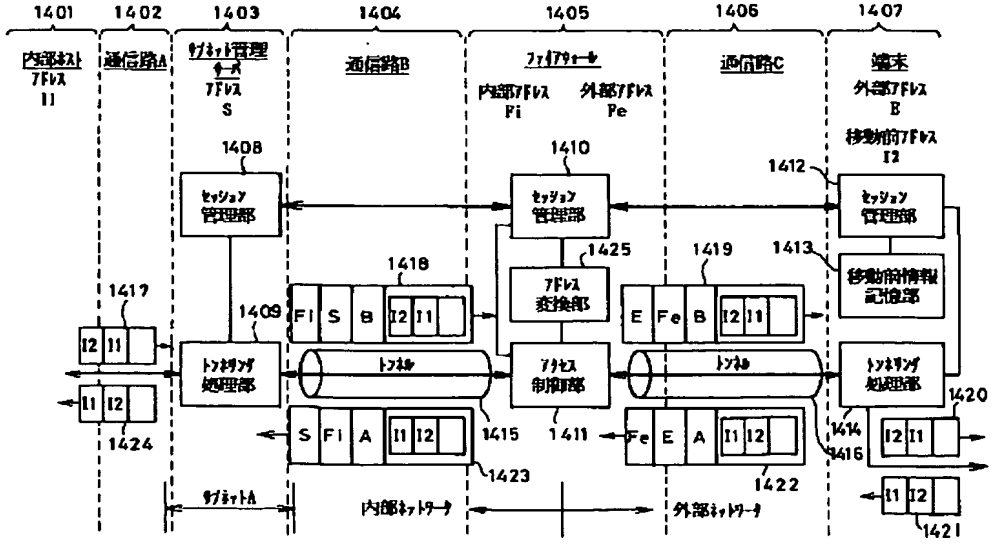
【図１２】


1201
1202
1203
1204
1205
1206
1207
内部ホスト
アドレス
I1
通信路A
サブネット管理
サーバ
アドレス
S
通信路B
ファイアウォール
内部アドレス
Pi
外部アドレス
Pe
通信路C
端末
外部アドレス
E
移動前アドレス
I2
1208
1210
1212
セッション
管理部
1225
1213
アドレス
変換部
移動前情報
記憶部
1218
1219
1217
1209
Fi
S
E
Fe
I2
I1
トンネリング
処理部
トンネル
アクセス
制御部
1220
1215
1211
1214
1216
1224
1223
1222
1221
サブネットA
内部ネットワーク
外部ネットワーク

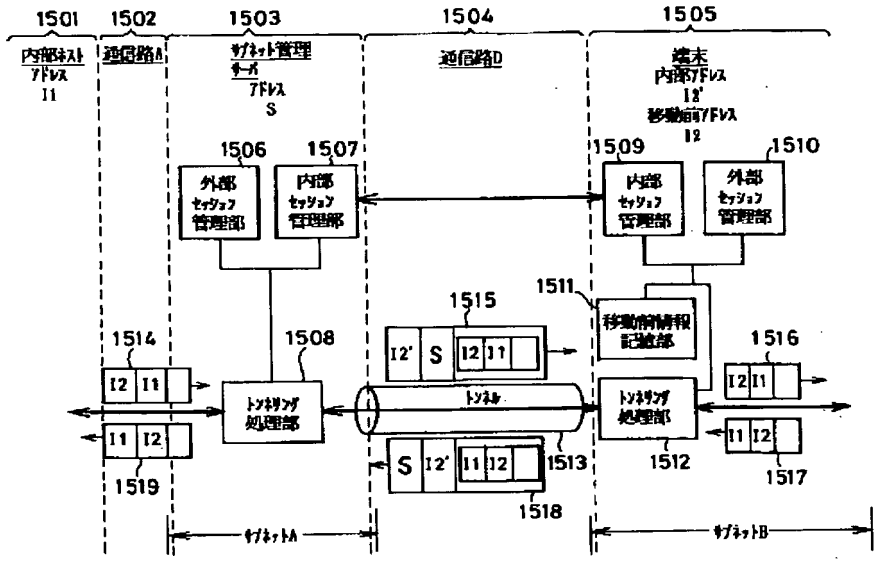
【図１３】


1301
1302
1303
1304
1305
1306
1307
内部ホスト アドレス I1
通信路A
サブネット管理サーバ アドレス S
通信路B
ファイアウォール
内部アドレス Fi1～Fin
外部アドレス Fe
通信路C
端末
外部アドレス E
移動前アドレス I2
1308
1310
1312
セッション管理部
1325
1319
1313
移動前情報記憶部
1318
1317
1309
アドレス変換部
トンネル
アクセス制御部
トンネリング処理部
1320
1315
1311
1314
1316
1324
1323
1322
1321
サブネットA
内部ネットワーク
外部ネットワーク

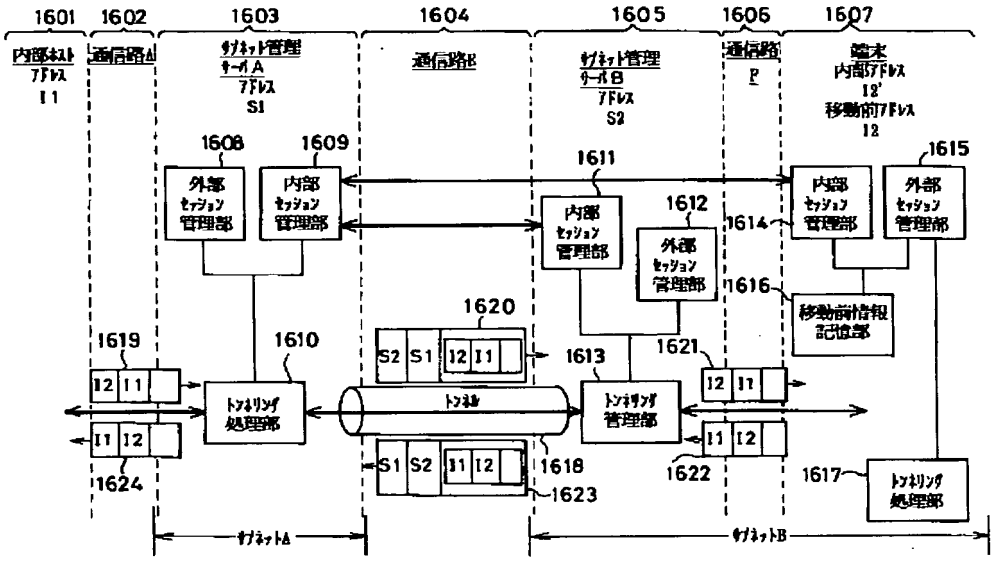
【図１４】


1401
1402
1403
1404
1405
1406
1407
内部ホスト アドレス I1
通信路A
サブネット管理サーバ アドレス S
通信路B
ファイアウォール
内部アドレス Fi
外部アドレス Fe
通信路C
端末
外部アドレス E
移動前アドレス I2
1408
1410
1412
セッション管理部
1425
1419
1413
移動前情報記憶部
1418
1417
1409
アドレス変換部
トンネル
アクセス制御部
トンネリング処理部
1420
1415
1411
1414
1416
1424
1423
1422
1421
サブネットA
内部ネットワーク
外部ネットワーク

【図１５】


1501
1502
1503
1504
1505
内部ホスト アドレス I1
通信路A
サブネット管理 サーバ アドレス S
通信路D
端末 内部アドレス I2' 移動前アドレス I2
1506
1507
1509
1510
外部 セッション 管理部
内部 セッション 管理部
内部 セッション 管理部
外部 セッション 管理部
1511
1515
移動前情報 記憶部
1514
1508
1516
I2 I1
トンネリング 処理部
トンネル
トンネリング 処理部
I1 I2
I2' S I2 I1
S I2' I1 I2
1513
1512
1517
1519
1518
サブネットA
サブネットB

【図１６】


1601
1602
1603
1604
1605
1606
1607
内部ホスト アドレス I1
通信路A
サブネット管理 サーバA アドレス S1
通信路B
サブネット管理 サーバB アドレス S2
通信路 P
端末 内部アドレス I2' 移動前アドレス I2
1608
1609
1611
1615
外部 セッション 管理部
内部 セッション 管理部
内部 セッション 管理部
1612
外部 セッション 管理部
内部 セッション 管理部
外部 セッション 管理部
1614
1616
移動前情報 記憶部
1620
1619
1610
1621
1613
S2 S1 I2 I1
I2 I1
トンネリング 処理部
トンネル
トンネリング 管理部
I1 I2
S1 S2 I1 I2
1618
1622
1617
トンネリング 処理部
1624
1623
サブネットA
サブネットB

THIS PAGE BLANK (USPTO)